O L L I   P I T K Ä N E N

LEGAL CHALLENGES TO FUTURE INFORMATION BUSINESSES

Helsinki University of Technology

Department of Computer Science and Engineering

Software Business and Research Institute

and

Helsinki Institute for Information Technology HIIT

P.O.Box 9800, 02015 TKK, Finland

Author: Olli Pitkänen

Name of the dissertation:
Legal challenges to future information businesses

Department: Computer Science and Engineering

Laboratory: Software Business and Research Institute

Field of research: Digital economy

Opponent(s): Professor Olli Martikainen, Professor Jukka Mähönen

Supervisor: Professor Martti Mäntylä

Instructors: Professor Jukka Kemppinen, Professor Juha Laine

Abstract
The thesis studies new legal challenges to future information businesses: it presents an applicable research method, lists central legal challenges, and discusses the implications of those challenges.
I have developed a scenario-based method that produces lists of legal challenges and helps to analyze them.
The method highlights information products and services from commercial entity's viewpoint: other business aspects are paid less attention. Also, some specific characteristics of particular companies cannot be considered in a general method like this. Therefore challenges in legal areas such as tax law or competition law do not appear although in practice they can be relevant. The method is still able to point out numerous relevant legal challenges.
The study focuses on the future: the time span is about two to ten years from now. The focus is on the business-to-consumer (B2C) market. The emphasis is on strategic product and service development.
I have listed, analyzed, and discussed the future legal challenges that the method has found. I conclude that the most important legal challenges to future information businesses are within the areas of privacy and data protection; intellectual property rights; and contracts. I have also discussed the major distinguishers of businesses implying legal challenges. They help to point out the specific legal challenges related to a certain information product or service.
Legal rules can affect businesses in many ways. At their best, they enable businesses, but too often they also harm useful activities. I conclude business drivers and hurdles that are important from the legal point of view.

Summary of Contents

Table of Contents

FOREWORD

I began to write this thesis during a research project on intellectual property rights related to content products and the Mobile Internet. Especially copyright was emphasized because of its significance for content production. The project took place in California from October 1999 till August 2000. I was employed by Helsinki University of Technology and hosted as a visiting scholar at University of California, Berkeley. The project was funded by Nokia Research Center and accomplished in cooperation with Nokia's personnel.

The work was continued in the follow-up project called *MobileIPR* at Helsinki Institute for Information Technology HIIT. Tekes, Elisa, Nokia, Sonera (now TeliaSonera Finland), L M Ericsson, and Yleisradio generously funded the project. MobileIPR was accomplished in 2001-2004. [122] During MobileIPR, I spent another year at University of California at Berkeley. After that, I have studied future legal challenges in several HIIT research projects, especially MobiLife (EU, IST-2004-511607), Wireless Festival (Eureka/Celtic CP1-019), and Mobile Content Communities MC2. Those projects formed a research environment, which provided me with supplementary and validating aspects.

I am a software engineer (M.Sc., 1994, and Lic.Sc., 2002, Helsinki University of Technology) and a lawyer (LL.M., 1996, University of Helsinki). I have worked as an engineer for IT companies like Hewlett-Packard and IBM. I have practiced law at Opplex Attorneys-at-Law, now Puiro Snellman Åkerlund Attorneys-at-Law. Also, I have participated in business strategy development processes as a board member of

IT companies like Nixu, Gaudeamus Data, and Bookit. Therefore, I have also personal experiences in issues I am writing.

An earlier version of this thesis was accepted as my licentiate's thesis at Helsinki University of Technology in 2002. It was titled *Managing Rights in Information Products on the Mobile Internet* and its aim was to describe a rights management framework for the Mobile Internet. [97] The main contributions in this doctoral thesis in comparison with the licentiate's thesis are the analyses of additional scenarios, the updated list of legal challenges, the list of major distinguishers of business models implying legal challenges, and the further analysis of those legal challenges and major distinguishers. I have also revised all the other parts of the thesis as well.

I have been privileged to work simultaneously under the supervision of several distinguished scholars. Professor Martti Mäntylä has been the supervisor of this thesis, the research director of Helsinki Institute for Information Technology HIIT, and the project leader of several research projects that I have worked for. I have been lucky to receive remarkable slices of his valuable time and I have gained a lot especially on his expertise on technologies. Without his guidance and support, the thesis would not be completed yet. Professor Jukka Kemppinen has been the responsible leader of MobileIPR project, he has been the instructor of this thesis, and he has contributed a lot to the actual research work. Professor Juha Laine, the second instructor of my thesis, was appointed to the professorship of digital economy at Helsinki University of Technology not until amid my research work. Therefore I have not been able to work with him all the time, but still his opinions have affected the thesis. Professors Jukka Mähönen and Josu Takala were the pre-examiners of the thesis. Their encouraging comments helped me to finalize the work. Professor Jukka Mähönen and Professor Olli Martikainen have kindly accepted to be the opponents in the public examination.

It is essential for a researcher to have colleagues with whom one may discuss and exchange ideas. During the years that I have worked on these research issues, I have had the pleasure to work with numerous proficient researchers, like Mikko Välimäki, Ville Oksanen, Tommo Reti, Aura Soininen, Perttu Virtanen, Risto Sarvas,

INTRODUCTION

BACKGROUND

At the time of writing this thesis, the business world is only slowly recovering from the economic depression that was largely due to the collapse of so called *dot.com bubble*. Afterwards, it is easy to be wise, know better, and find the causes of problems. However, it is more important to look forward: what can we do to avoid similar problems in the future? This thesis is answering to a small subtlety of that incredibly wide question, namely how assessing legal challenges can help to make a future information business more successful or at least to facilitate avoiding failure.

Legal challenges, in this thesis, refer to difficulties in legal reasoning or somehow unsatisfying outcome of the legal process. In general, legal structures enable business, but they may also constrain possibilities. Laws make it easier to anticipate the future legal conditions. For example, it is hard to foresee how a contractual relationship is assessed legally if there is no governing law. For that reason, legal structures generally diminish risks and thus enable business. Then again, legal structures may also constrain and harm business. Although some of the constraints are due to rules that positively prohibit certain actions, many of them, in fact, are results from the lack of enabling legal structures.

Legal constraints are not necessarily absolute obstacles, but may still pose noteworthy risks. An obstacle refers here to something that prevents an entity from doing certain information business. For example, the European Directive on the protection of personal data (Directive 95/46/EC) bans certain usages of personal

information. A business that would essentially be based on such a usage is thus prohibited. In other words, there exists a legal obstacle. On the other hand, uncertainty that often relates to decision making is hardly an obstacle, but rather points to risks. Therefore assessing legal constraints is closely related to risk management. [35, 94]

Laws do not usually change the way technology advances. There are some exceptions though. For example, safety and environmental regulation may force industries to develop technologies that fulfill new regulation; automobile industry has had to develop low-emission technologies to adjust to new legislation. A recent example is a US court case *Lexmark v SCC* in which the judge pointed out that intellectual property rights may lead companies to develop unnecessary technologies to avail of IPR protection and thus limit competition. Judge MERRITT: "If we were to adopt Lexmark's reading of the statute, manufacturers could potentially create monopolies for replacement parts simply by using […] lock-out codes. Automobile manufacturers, for example, could control the entire market of replacement parts for their vehicles by including lock-out chips." [165]

In certain areas, like privacy and data protection as well as products liability and quality engineering, laws may also force entities to improve their products to better protect end-users' privacy or physical safety. Both privacy and products liability regulations are often claimed to be too strict and harm businesses. In some cases, this may be true, as discussed further below, but in countries, in which exist e.g. strict products liability laws, entities rapidly try to make their products safer, when a defect is found. The end-users themselves are hardly able to force the producers to better the products without such support by laws. End-users' awareness and negotiation power are not always sufficient.

The underlying viewpoint in this thesis is that anyone who wishes to do business that is related to information products or services should consider legal challenges. Then again, it depends on the business strategy how much one wants to invest in managing those risks. This thesis aims at giving justified means to decide how to strategically plan business and manage risks related to legal challenges.

SCOPE

VIEWPOINT

The focus of the thesis is on *businesses*, i.e. commercial enterprises. Public entities, non-profit organizations, communities, and consumers are of course also relevant and they affect a lot on these businesses as customers, authorities, partners, and so on, but their special needs and challenges are not in the focus of this thesis.

Therefore, many interesting legal challenges related only to the non-commercial avail of information are left out. For example, copyright is often divided in economic rights and moral rights. Economic rights are most important to commercial actors while moral rights are of lesser importance. Thus the emphasis in this thesis is on the economic side of copyright. Then again, although for example privacy does not directly protect commercial entities, they have to consider their customers' and end-users' needs and thus privacy is a central issue in the thesis.

Public libraries are especially in Finland significant with respect to information products and services. However, they are not commercial and thus mostly out the scope of this thesis.

My focus is on legal challenges. Therefore, I exclude risks and challenges, which can be related to innovation processes, but which are not legal. That is, I am not covering normal business risks, risks related to changing markets, risks in new technologies themselves, and so on.

INDUSTRY

The focus is on *information* products and services. Therefore especially the entities that actively participate in the content production value networks, i.e. produce, edit, aggregate, filter, publish, distribute, retail, promote, or deliver information are within the scope of this study. Not only content products, but also

software and metadata are information. Therefore also software companies and businesses that specialize in enhancing content with metadata are in the scope.

In contrast, businesses that do not directly add value to information products and services are excluded from the scope. Especially, entities that simply transfer data ignoring the information that the data may carry are not in the focus. For example, telecom operators are currently seeking their natural positions in the market. Some of them are merely providing infrastructure, acting as mere conduits. They are excluded from this work. Most operators on the other hand strive after value-added information services, which are included in the scope of this study.

A device manufacturer does not seem to provide information products – although major parts of many devices nowadays are software and information – but might benefit from supporting information businesses in solving legal challenges. For example, by adding suitable features to a mobile device, it could be made easier for an end-user to control private information, which in turn would make certain information services legal and profitable. Therefore, a device manufacturer is not in the focus of the thesis, but it could benefit from taking these issues into consideration.

TIME SPAN

The thesis is about the *future*. It is probably not necessary to define the time frame exactly, but I am focusing on a period that will begin after about two years from now and end after about decade. Before that, nothing much has changed and the futures research method that is used in this study is hardly applicable. I am not emphasizing legal challenges that are already common today. After ten years, technology has probably developed so much that it is difficult to say anything about information businesses of that time.

Because of the time span, conventional jurisprudence or legal science, especially legal dogmatics is of limited use in this study. From the methodical viewpoint, legal dogmatics is hardly able to tell us about the future – or even about the present, for

that matter. It focuses on how the things *ought to be*, not how they are or will be. Jurisprudence fetches information from the reality and forms a normative system or a framework on top of real phenomena. Legal scientists are mainly focusing on the positive study of actual law (*de lege lata*), and somewhat discussing what the law ought to be (*de lege ferenda*). Yet, jurisprudence, especially legal dogmatics, does not provide the scientist with tools to analyze the future circumstances, subjects, relationships, and environment in which the law will be applied.

Legislators are frequently producing new laws. One might say that the legal system is changing rapidly. Yet, it takes time to make profound changes in legal systems in modern western societies. The whole legislative process, preparation, committees, drafting bills, passing the law in the legislative body, and finally bringing the law into force, takes years. If there are international aspects or the area belongs to e.g. European legislation, the process lasts even longer. Certainly, small changes to existing laws can be made rapidly, but large reforms are slow. Thus, in the given time span – in the next ten years or so, it is unlikely that the legal system would change remarkably. Therefore, in this study, I am able to suppose that the laws are quite static. In that sense, I am studying the issues that will appear if the laws will not change, but the phenomena, to which the laws are applied, will keep changing. From the legal science's point of view, I am studying how the existing laws (lege lata) work in the changing conditions, although in conclusions I am also able to discuss a little what the laws ought to be (de lege ferenda).

MARKET

The thesis concentrates on *B2C*, i.e. *business-to-consumer* information businesses. Often the same issues arise also in B2B (business-to-business), C2C (consumer-to-consumer), P2C (public-to-consumer), and so on, and obviously even in a B2C information business value chain, there usually exist also B2B relationships. However, the focus is on B2C, and less attention is paid to other models.

Consequently, legal issues related to settings in which a few competing commercial providers try to sell their products and services to numerous individuals, families, and user-communities are essential. In this kind of a situation, unlike in many B2B cases, it is not usually practical to make separate agreements with each customer – the transaction costs would become too high. Instead, the seller needs to rely on mass contracts, i.e. use standard terms and conditions with all the customers, or the legal relationship between the seller and the customer is to be based on legal rules, like copyright law or consumer protection law. Electronic agreements may change this somewhat: standard contracts can be increasingly automatically "mass-customized" in accordance with a certain customer's specific needs, but this is not likely to prevail in the next decade.

INNOVATION PROCESS PHASES

The focus is on *strategic product and business planning and development.* Product development and innovation processes essentially aim at searching ideas and identifying customer needs, stating product specifications, generating, selecting and testing concepts, defining product architectures, creating industrial design for manufacturing, and prototyping. Throughout the process, ideas and concepts are filtered, rejected or postponed (go/no-go, kill/hold/proceed, etc.). At least ideally, the process should gradually select and refine the raw ideas, particularize plans, and increase the organization's understanding on the issues so that finally the best ideas are developed into commercial products. It is important to be able to kill the inviable ideas as early as possible to avoid unnecessary investments. Therefore the legal challenges that may severely affect on the viability of the product should be noticed in the early phases of the process. [129]

There are many kinds of legal challenges. Some of them are severe. They can be obstacles, that is, they can prevent certain information businesses. Some of the legal challenges – even if they do not prevent the business – may significantly affect the investments, costs, or profit expectations. Those obstacles and significant challenges should be noticed as early as possible so that they can be assessed together with

other strategic factors. For example, one of the well-known model product development processes is the Stage-Gate process. It consists of five gates and five stages. The assessment of legal challenges should be accomplished mostly during the first two stages, because it is comparable with patent & IP search, competitive alternatives assessment, commercial application outline, and building the business case. [23]

The research projects, in which I have recently applied the method that I present in this thesis, are grounded on the user experience basis. In the beginning of a prototype development, a user study is conducted and some product concepts are created on that research work. The prototype is developed to implement a selected concept. This process is based on User-Centered Product Concept Design model or UCPCD. [56, 57]

The user-centered product concepts are created in the very beginning of product development process and thus they can be compared to the early stages of the Stage-Gate process above. The concepts are attractive candidates to be analyzed from the legal challenges viewpoint since they present phenomena that are easy to assess legally. However, they also have significant limitations because they do not usually express business issues. [56, 57] Many legal challenges are hidden until it is expressed how the businesses are to make profit in the case. Therefore, it would be helpful to elaborate concepts further to get the full picture of all the important legal challenges. Especially, a reasonable business analysis is needed for a comprehensive legal analysis. I have not been able to complete this so far, but comprehensive business analysis remains to be accomplished in the future studies.

On the other hand, as the understanding of the details of the concept increases during the product development, also more legal challenges can be found. Some of the legal challenges are not visible in the early phases of the development process. For example, defining commercial product possibilities in a later phase may bring out new legal challenges. Therefore the assessment of legal challenges should not be done in the beginning of the development process alone, but the challenges need to be reassessed repeatedly.

On the other hand, my practical experience suggests that often the legal analysis is done only in a late phase of product development, when a lawyer is asked to check that everything is alright. At that point, the lawyer has little time to react, and few possibilities to change anything. If any severe legal problems are found, the lawyer can usually only ask the project to be cancelled or try to minimize damages with contractual arrangements. Surely, it would help if legal analyses were made earlier. Ideally, assessing legal challenges is a continuous part of the innovation process.

However, in this thesis, I am focusing on the strategic legal challenges that need to be considered in the early phases of product and service development. Also, the time span defined above, two to ten years from now, suggest that the focus is on the early phases of the product development, or even before that – namely in research activities that precede product development. I exclude the assessment of legal challenges in the later phases of product development and thereafter. The detailed analysis of those legal challenges that can be taken care of in the latter phases of product development process and the challenges that are not visible in the early phases need somewhat different approach. The details of laws and all the special characteristics of the case need to be considered. They can usually be managed using contracts and by fine-tuning technical and business solutions. [23]

Because I am focusing on strategic planning and product development, I am studying legal challenges on the quite high level of abstraction. I am mainly not discussing the details of certain statutes, but focusing on pointing at the legal areas in which the significant legal challenges can be found. I am keeping off the full details of legal provisions.

To concentrate on the early phases of innovation process, it may exclude some legal areas as such. For example, businesses in general try to achieve as strong a position in the markets as possible. They use progressive products and services, marketing measures, legal means including intellectual property rights and contracts, and so on. Yet, an entity's actual position in the market depends fundamentally on the success of the innovation process. Therefore, legal challenges related to competition law are largely invisible in the early phases of innovation process.

For example, the core issue in the antitrust trials against Microsoft has been bundling. The question is why Microsoft may not integrate a media player or a web browser into the operating system, and why Microsoft must provide a way to remove bundled applications. Apple and other operating system manufacturers are also tightly integrating similar programs into their systems, but they are not sued. Why not? The main difference between Microsoft and Apple is their market positions and how they use or abuse their standings. In a nutshell, it is not because of bundling itself why Microsoft was sued. Nor is it Microsoft's monopoly position. Instead, it is the illegal use of that position to maintain and extend Microsoft's power into other markets. Therefore other operating system makers – like Apple – can get away with integration and bundling, whereas Microsoft cannot. Also, Microsoft can start developing new products without concerning competition law until it considers how the new product is positioned in the markets and how Microsoft uses its power in relation to that product. These decisions are typically not made in the early phases of product development, because the actual competitive circumstances will not be revealed until later.

The real importance of competition and antitrust law depends not only on what kinds of products, services, and technologies will be available and how they are bundled, but on which companies are dominant players in the markets and how they behave. Competition law applies economic science in general to the foreseeable future, but it is always related to the market situation and changes dynamically. The scenarios do not present market situation. That is why it is hard to foresee what sort of effects competition law actually will have. Although competition law is important and highly interrelated, for example, to intellectual property rights, it is not possible to analyze it in detail in this study.

Obviously, companies are largely able to predict their future positions based on their current positions, strategies, and general foresight. Therefore, in a concrete business case, it is probably possible to identify challenges also in the area of competition law. In this thesis, however, I am not able to point at challenges in competition law, which affects future information businesses at large.

MEDIA

The *Internet* – both wired and wireless – will be the central media to distribute information in the future. Therefore, the Internet is in the focus of the thesis. Other technologies that are relevant but not in the focus include e.g. off-line media (like DVD) and other on-line networks, like GSM or 3G mobile networks and digital broadcast networks. Mobility is dramatizing issues in networks. Therefore I emphasize mobility and often refer to the Mobile Internet, although it will probably not prevail in 10 years. [75]

Because I am emphasizing the Internet and mobile networks, it makes certain legal aspects especially important. For example, as further discussed later, network technologies release users from many geographical limitations. Legally, this introduces challenges since legal systems have traditionally been very location sensitive: jurisdictions are often defined by geographical boarders. In the similar way, the easy access to information and the sharing of resources through networks and resembling network-related phenomena highlight specific legal issues, and thus color my thesis. [35]

RESEARCH QUESTIONS

The questions I am answering in this thesis are especially the following:

How to study future legal challenges? Within the scope defined above, how to point at the legal areas in which the most critical legal challenges are? What are the limitations of the method? What sorts of challenges remain unnoticed? To study future information businesses is unavoidably cross-disciplinary task. Therefore one of the major questions is what methodologies to use and how to study this area.

What are those legal challenges? Which of the challenges are the most important? What kind of distinguishing factors in businesses mostly affect or cause the challenges? The first outcome of the study is to be a list of central legal challenges categorized by legal areas.

What are the implications of those legal challenges? How they affect businesses? Why product development should care about legal challenges – also other than those related to patents? Is there something that legislators should do? To further improve the results, the list of challenges is analyzed and the implications of those challenges to businesses are discussed.

RELATION TO OTHER WORK

This thesis is not completely inside one single well-defined field of science. Instead, to position this work in relation to others, I need to briefly discuss several areas. Especially, the following have strong connections to my work:

- Legal science
- Futures research
- Strategic management
- Product development research

LEGAL SCIENCE

Legal science is the "field of study that, as one of the social sciences, deals with the institutions and principles that particular societies have developed (1) for defining the claims and liabilities of persons against one another in various circumstances, and (2) for peaceably resolving disputes and controversies in accordance with principles accepted as fair and right in the particular community at a given time." [36]

The subject of this thesis is closely related to legal science. Legal challenges in this thesis refer to difficulties in legal reasoning or somehow unsatisfying outcome of

the legal process. Legal reasoning and legal processes are also subject matters of legal science as defined above. However, what separate this work from legal science are the methodology and the time span.

Any scientific method is heavily influenced by what are the sources of scientific information in that field of science. The *doctrine of sources of law* defines on what judicial decisions may be grounded, and it significantly limits on what legal studies, especially *legal dogmatic research*, can be based. AARNIO [2, 3], DWORKIN [30], KELSEN [59], and other traditional legal scientists have studied where the judge obtains the rules by which to decide a case. Usually the sources of law include statutes, custom, preparatory works, precedents, jurisprudence, legal principles, morality, and real arguments. Although different legal systems have slightly different emphasizes and they change in the course of time, statutes, customs, preparatory works and precedents usually have most impact on legal reasoning. By their nature, they reflect past and not foresee the future. Principles, morality, and real arguments, which may also take forthcoming circumstances and consequences into account, appear less in court decisions and legal studies.

Recently many legal scholars have developed methods that are less dependent on the doctrine of sources of law. Typically they emphasize that, when applying the law, one should add weight to issues that are not on a high level in the traditional hierarchy of sources of law, but merely considered principles or real arguments. In Finland these modern approaches include e.g. KARHU's new property law, risk positions, and the dynamic interaction between economy and law [3, 104, 105]; and WILHELMSSON's social civil law, welfarism, and social justice [133]. They are related to international movements like *critical legal studies* (CLS). Also, one of the most significant movements in legal science has been *law and economics*, which aims at studying legal questions using economic methods. [24, 83] Yet, none of these approaches or movements tries to change the fundamental approach that legal science is to interpret existing law, not to foresee the future.

In legal science, it is typical to make a distinction between *ex post* and *ex ante* approaches. The ex post perspective is backward looking. It is based on knowledge

and fact. A court normally uses ex post reasoning, when it answers to questions like, who acted badly, who acted well, and whose rights were violated. In contrast, the ex ante perspective is forward looking. It is based on assumption and prediction. A policy maker hopefully considers questions like, what affect this rule will have on the future, and will the proposed regulation produce good or bad consequences. [36]

In property law, according to KARHU, it is important to separate the inspection of the appraisal of liability ex ante and ex post. Ex post approach dominates in juridical analysis and decisions. The distinction is, however, more fine-tuned. For example, the matter of liability is often decided based on foreseeability, that is, depending on whether the consequences were ex ante reasonably anticipable. The notion of time that the distinction between ex ante and ex post contains is discovered when it is noticed that one arrives at ex ante moment from the consequence moment. Ex ante moment is not chosen independently, but it is defined by the judge's subsequent analysis ex post. [103]

In jurisprudence, the concept of ex ante therefore typically refers to past foreseeability: what someone should have been able to foresee. Alternatively, it may also refer to policy issues: what sort of rule makes a better future. It differs, however, from the method in this thesis since it does not refer to the future legal challenges of a certain entity. On the other hand, the legal analysis of the future scenarios in this thesis is accomplished using legal science approach. Therefore, even if the thesis does not belong to legal science, it is directly linked there.

FUTURES RESEARCH

According to BELL, futures studies "involves systematic and explicitly thinking about alternative futures". [14]

According to MANNERMAA, a "futures study has a certain interest of knowledge of the future in the sense that, on the basis of the study of the present and the past, one is presenting well-argumented assessments of the future. The purpose of these arguments is to offer a basis for societal planning and decision-making activities as

well as for the more general citizen's discussions and activities which are taking place at present." [74]

In recent years, futures research or futures studies has established itself as a respected field of science. Although it is impossible to receive direct information from the future, it is possible to study what kinds of alternative futures are possible, which paths lead to certain futures, and how people can affect on those paths and futures. Futures research provides us with a large toolbox of methods that can be applied in other fields of science. Those methods include trend analysis and extrapolation, Delphi methods, cross impact models, world models, technology forecasts (S-curves, technological substitution, diffusion models), technology assessment, analogies, strategic scenario approaches, soft systems methodology, megatrend analysis, and monitoring of weak signals. Social sciences, economics, business research, and environmental research among other have availed extensively of futures research methods. On the other hand, futures research can hardly be an end in itself. The value of futures research depends on how much useful information it can produce for the other studies. In this thesis, futures research is an invaluable source of information. It provides methods and ideas on how to study the future legal challenges. [14, 16, 74, 98]

STRATEGIC MANAGEMENT

According to MINTZBERG, AHLSTRAND, LAMPEL, *intended strategy* refers to a plan and *realized strategy* is a pattern, i.e. consistency in behavior over time. Fully realized intentions are *deliberate strategies* and those that are not realized at all are *unrealized strategies*. In *emergent strategy*, a pattern realized was not expressly intended. However, all real-world strategies need to mix these in some way to exercise control while fostering learning. [79]

Strategy can refer to a *position* – to the locating of particular products in particular markets. According to POTTER, strategy is the creation of a unique and valuable position, involving a different set of activities. [101] Yet, strategy can also be

seen as a *perspective* – an organization's fundamental way of doing things. Strategy can also be a *ploy* – a specific maneuver intended to outwit an opponent or a competitor. [79]

In this thesis, I am focusing on future challenges. From the strategic management viewpoint, this focus emphasizes planning and intended strategy. Although business lawyers are often regarded as plotters, the intention of this thesis is not to provide clever ploys but merely help strategic management to define the company's perspective of handling the future legal challenges.

On the other hand, in this thesis, I am not able to consider the specific strategic challenges to a certain enterprise. Merely, I need to concentrate on more general, industry-wide issues. Therefore, factors like market position or organizational culture, which are quite special to a particular entity, cannot be considered here, even if they may have significant effect on legal challenges.

PRODUCT DEVELOPMENT RESEARCH

The subject of the thesis is closely related to product development research, since I am focusing on the strategic product and business planning and development as discussed above. Large amount of literature covers product development and innovation processes extensively (see for example, ULRICH & EPPINGER [129]; COOPER, EDGETT & KLEINSCHMIDT [23]; and KANKAINEN [56]). It seems, however, that they have hardly discussed other legal challenges but intellectual property rights. It is typical to warn companies not to infringe others patents and to protect one's own inventions. Therefore, the publications on product development frequently make references to patent law, but the other fields of law are mostly ignored. (Interestingly, KANKAINEN briefly mentions privacy as an ethical issue that calls for further research and discussion. [56]) From my perspective, patent law represents a narrow, yet of course an important approach to legal challenges. My intention is to broaden the view and give product development reasons for considering also other legal challenges in addition to patents.

STRUCTURE OF THE THESIS

The thesis is organized as follows:

In *Introduction* I am motivating the study, giving background information of the subject, defining the scope, and orientating the reader to the approach, the view points and the research questions of the thesis.

Terms and concepts are often ambiguous. There are hardly correct meanings, but it is important to understand at least approximately, what the author has meant by certain words to understand the message that is tried to be communicated. In *Definitions*, I am first giving my explanations to certain *central concepts* that I am constantly using in the thesis. Then I am presenting some legal terms that have more or less established interpretation in legal language. This *legal glossary* is intended especially for non-lawyers to help them wade through the legal parts of the thesis.

In *Methods*, I am explaining and giving reasons for the research methods that I have used in this thesis. I have constructed a method to study future legal challenges. For this constructive part, I have gathered requirements from the introduction part of the thesis. The topic is cross-disciplinary and focuses on future issues. Therefore I am applying futures research scenario methods, but also legal analysis while referring to authors in multiple fields of science.

In short, I am first discussing the factors that affect the legal challenges to future information businesses: *socio-economic viewpoints* and *technological advances*. They are to be the *Factors to Scenarios*. Then I am studying the most important attributes of those factors.

To make the study more concrete, I am giving a few *Examples of Information Businesses*. They are to demonstrate especially the technological development but also give some thoughts of business opportunities.

Next, I present a few sets of *Scenarios*. First, I am describing a set of micro scenarios that I have created and that illustrate the factors and their attributes. I am also presenting the legal analysis of those scenarios. The second set includes

scenarios that others have created, but I have analyzed to control the results that my own scenarios brought up. The third set of scenarios consists of macro scenarios that describe the development of the society at large. Based on the legal analysis of all of these scenarios, I am ready to list the legal challenges and to identify the legal areas that seem to have most open issues in relation to future information businesses.

Legal Implications include further analysis and discussion on the legal challenges that were identified in the previous chapter.

In *Conclusions*, I discuss the results of the thesis and the future work.

DEFINITIONS

Many terms and concepts in this field are quite ambiguous and vague. Numerous buzzwords without proper definition occur frequently even in scientific papers. It seems that today almost everything has an e-, m-, or u- prefix or an attribute *digital* without explanation. The prefix "e-", for example, should mean *electronic,* but it does not necessarily mean that the issue in question has anything to do with electricity. Digital on the other hand should refer to digits, but often digits are not essential properties of those "digital" matters under discussion.

A good example of the rhetoric in this field is the name of the controversial U.S. copyright statute "Digital Millennium Copyright Act", DMCA [155]. According to Random House Webster's Unabridged Dictionary, *millennium* may refer to "a period of general righteousness and happiness, esp. in the indefinite future". [106] Obviously, it is digitalization that brings forth this happiness and DMCA is to protect it from evil pirates and infringers.

Of course, words can have several correct meanings, different disciplines may well use them in other senses, often the level of abstraction we are discussing also has an effect on what we mean by words, and the context and the domain of a discussion topic may affect the meanings also. However, careless and extensive use of hype-words makes it often difficult to understand the essential message. A careful reader will find these peculiarities in this thesis also. However, I have tried to use words in a consistent way and give an explanation when needed.

Below, in Central Concepts, I give my definitions of some of the important terms that occur regularly throughout the thesis. In the next subchapter, Legal

Glossary, I am presenting concepts that have a special meaning in the legal terminology. That is intended to help especially the readers that are not too familiar with legal language.

CENTRAL CONCEPTS

Information is stimuli that have meaning in some context for its receiver. Information can be converted into data and passed on to another receiver. Relative to the computer, we can say that information is made into data, put into the computer where it is stored and processed as data, and then put out as data in some form that can be perceived as information. [191]

Data are numbers, characters, images, or other method of recording, in a form which can be assessed by a human or especially input into a computer, stored and processed there, or transmitted on some digital channel. Computers nearly always represent data in binary. Data on its own has no meaning, only when interpreted by some kind of data processing system does it take on meaning and become information. People or computers can find patterns in data to perceive information, and information can be used to enhance knowledge. The Free On-line Dictionary of Computing gives us an illustrating example: "1234567.89 is data. 'Your bank balance has jumped 8087% to $1234567.89' is information. 'Nobody owes me that much money' is knowledge. 'I'd better talk to the bank before I spend it, because of what has happened to other people' is wisdom." [177]

Another way to illustrate how data differs from physical medium and information is to imagine text in a piece of paper. If the text is looked close enough – using a microscope or a magnifying class for example – one can see the details of the surface of the paper and ink on it. That is physical medium. When the viewer grows away from the paper, single characters or letters can be seen. That is data. When the distance increases further, one can see words, sentences, and paragraphs and starts to understand what the text says. That is information. By processing this information in the brains, the reader gets knowledge and maybe ultimately some wisdom.

While I try to use the words consistently, I sometimes – even deliberately – make exceptions and use words, for example, data and information in different meanings. For example, it is customary to call the protection of private information *data protection* and, for instance, the EU directives call personal information (e.g. information on person's location) *personal data* (e.g. *location data*). Although, in accordance with my definitions above, I should call them information, I am also using word data to be consistent with the references and the other authors. It is not easy to use the words completely consistently even within one discipline – within multidisciplinary areas, like the subject of this thesis, it is impossible. [146]

An *information product* consists of valuable information, which is technically stored in a form that can be controlled and transferred between entities. It may include contents, metadata, and computer programs. [93]

An *information service,* in contrast, is an information supply in which information is processed for a user or provided on user's demand. It is often difficult to make distinction between the concepts of *product* and *service.* Many products can be *customized,* and they can be enhanced by included services. Then again, companies can *productize* their services, or take an otherwise generic type of service or support offering, and redefine and package it more as a product offering. [100] A supplier may want to productize its services to make management easier, but still give customers an impression of individualized services. The same object may be a product or a service depending on the view point. This makes the line between products and services even fuzzier.

Product has typically referred to tangible goods that are reproduced in quantity while a service has usually been work performed for the benefit of others. In the digital world, these kinds of definitions are clearly insufficient. Information products are not tangible goods. However, they may be reproduced in quantity. In this thesis, the word *product* refers to objects that are reproducible and packaged in a way that they can be delivered to multiple users. A *customizable product* is a product that can be adapted for users. A *service* refers to objects that involve significant work, either by human beings or by machines, for each user. Product and service are not mutually

exclusive concepts: an object may include both product and service components, and their weight depends e.g. on the viewpoint.

A *legal product* is the combination of the parts of a certain information product that are protected by legal rights in a certain jurisdiction at a certain time. Those parts that are protected by legal rights are called *legal components*. A legal component itself can be a legal product or an *atomic subject matter*. [93] These concepts could be visualized as if "legal light" illuminates an information product; those parts that are not protected by any legal right are transparent and cannot be seen. From the legal point of view, they do not exist. Legally, only the protected parts exist, or they are "visible in the legal light". If we further imagine a "shade", a certain jurisdiction at a certain time behind the information product, the "shadow" of the information product in the "legal light" on the "shade" is the legal projection of the information product or the instance of legal product in that jurisdiction at that time.
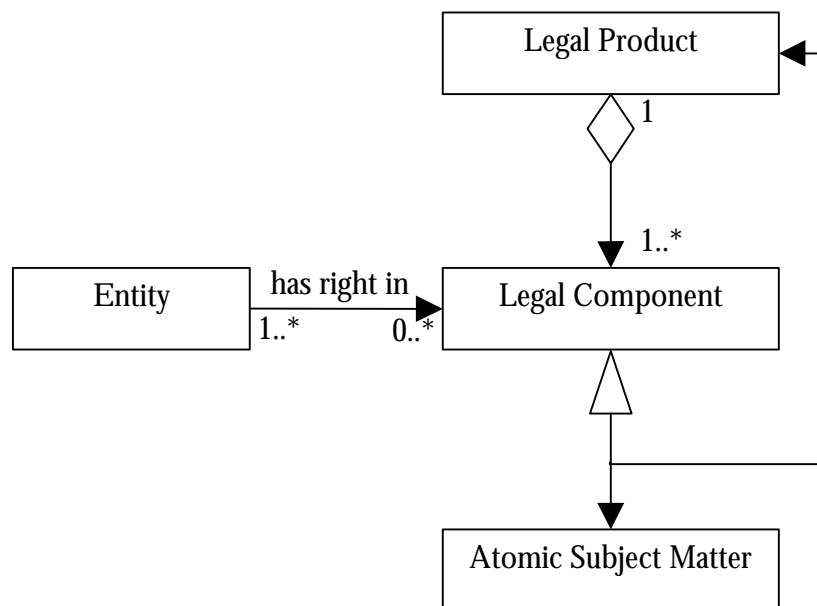
Figure 1. A legal product is the combination of legal components.

Figure 1 above illustrates in UML notation how a legal product is the combination of one or more legal components. An entity can have rights in legal

components that are either legal products themselves or atomic subject matters. On the other hand, several entities can have rights in a same legal component. This means that a legal product can be a complex combination of many kinds of legal components and the different rights of a number of entities in components. In general, a rights management system should be able to handle such complex legal products.

Content is the part of an information product without which the product has no value. The other parts, like metadata or programs, however, may add value to the content. It is not possible to precisely define the concept of content. As there can be tremendously many kinds of information products, also content can differ a lot. It can be nevertheless described as the actual payload of the information product. For example, a computer program as such can be an information product. On the other hand, as a part of a multimedia product, it does not necessarily need to be something without which the product has no value, but is merely a value-adding auxiliary part. Therefore a program may or may not be content.

Metadata is information about information. In information products, metadata is the part of the product that describes the content, its usage, tools or so on, but is not a program. Keeping in mind, how information and data have been defined above, it would be more appropriate to call it metainformation. However, metadata is such a well-known term that I use it in this thesis also. [54, 55]

A computer *program* is a specific set of ordered instructions or statements that is intended to be used in a computer to make the computer to perform certain actions or to bring about certain results. [155, 191] This kind of definition seems to refer to the machine-readable and executable program version, to the set of zeros and ones that is loaded into the memory of the computer and that the processor executes instruction by instruction. The fact is that only the executable set of instructions or statements actually makes a computer to do something. Nevertheless, it is not a big mistake to make the definition a little broader: a program can refer also to source code, bytecode and so on from which the executable program version is automatically compiled or which is executed by an interpreter, a virtual machine or

alike. Although a processor is hardly ever capable of executing source code directly, the relation between source code and executable code is such straightforward that it is reasonable to include source code into the definition. Most programs include errors that make at least some of the actions and results unattainable. Therefore I emphasize that in this definition the intention is significant, not the results. However, a set of instructions or statements that includes so many errors that it is not capable of performing anything intended is hardly a program, although it is hard to draw the line between programs and non-programs that way.

Software refers to all the information that is produced during a *software process*, i.e. during the process that is intended to produce a certain computer program. [10, 42, 102, 123] Software includes not only the program but also its documentation, database definitions, and so on. It should be noted that there are also many other kinds of definitions for software. For example, software may refer to the variable or the intangible part of a computer system while hardware refers to the invariable or the material part. [191] In this thesis, nevertheless, I prefer the first definition.

Digital Rights Management (DRM) refers to copyright technical protection. Earlier, I have tried to advocate that DRM should not be defined that tightly, but it should also include many other management related activities. Furthermore, it should not also be restricted to copyright or even to intellectual property rights, but *rights* should refer to other rights related to information products as well. In addition, if someone chooses to have a policy – for example – not to protect information products technically, in my opinion, that decision is within digital rights management also. The term "*digital rights management*" is also somewhat misleading in the sense that rights are not digital. In general, they do not have much to do with digits, but they are rather analog. The word "digital" refers supposedly to the subject matter, to information in digital form, not to rights in that information. It is also possible to think that the word "digital" refers to the fact that digital information technology is often used to manage the rights, "the digital management of rights" instead of "the management of digital rights". Yet, DRM does not refer to computer-aided rights management in general. For example, an investor can have a computer-based system to manage real estates, securities, contracts, etc., but this system is not called DRM. However, as it

has become evident that the meaning of DRM has been established, I give up: in this thesis DRM refers merely to the technical tools or measures that are intended to protect entities' copyright in information products.

LEGAL GLOSSARY

This chapter intends to give an overview of legal concepts that are used in connection to future information products and services. The emphasis is on the Finnish legal system – presenting the harmonizing European regime – and partially on the US legal system. The legal rights related to this area are numerous. It is not possible to cover them all in detail. I will only describe selected terms that are especially important from the perspective of this work.

An *entity*, in this thesis, is a person, a company, or any organization that may own rights.

An entity may have several different legal rights in one product and different entities may have rights in the same product. Those rights can be overlapping and protecting the same parts of the product, though in principle different rights protect different valuable parts of a product. For instance, patents can protect new, non-obvious ideas related to a product, copyright protects the way ideas have been expressed, trademark protects e.g. brands, and trade secret protects business information that is kept confidential to maintain an advantage over competitors.

In principle, information businesses should not concern legal rights only. An entity might have for example moral rights that are not legally enforceable. An entity may also believe that it has a certain right and act according to that although it actually does not have the right. Those moral and imaginary rights should be considered also, because they have an effect on how an entity manages its rights. Having said that, it is not in the scope of this thesis to discuss them further.

Cross-boarder issues and International private law

Large computer networks, such as the Internet, are fundamentally international. Communications technologies are largely neutral to geographic and territorial facts. Borders of countries have hardly any significance for data that is transferred on the network or for the devices that are connected to it. In contrast, legal systems are highly depending on territories; crossing a national border usually implies to the change of applicable laws.

International private law (or private international law or jus gentium privatum) informs us, which of the conflicting national laws is applicable, and usually also which nation's courts are competent and which national authorities may enforce a court's judgment. It refers to the set of legal rules governing international relations between private entities. Actually, international private law is not international in a same way as public international law is: a supranational set of rules that bind all the countries. No, international private law is merely a part of each legal system's private law. Therefore, even international private law varies in different countries. In German and Portuguese law, for example, it refers solely to the rules on conflict of laws, whereas in other systems it includes the rules on international jurisdiction and the recognition and enforcement of foreign judgments. All these rules relating to the applicable law, international jurisdiction and the recognition and enforcement of foreign judgments provide solutions to the difficulties that can flow from the fact that a single case can involve several separate legal systems. An example might be the case of a married couple of mixed nationality who are thinking of divorcing: in which countries their marriage is recognized, which court will have jurisdiction to order the divorce, and which laws will it apply? [35, 36, 176]

Privacy

In legal science, privacy refers to the protection of everyone's private life, honor and the sanctity of the home. It includes the secrecy of correspondence, telephony and other confidential communications; the protection of people's physical selves; the setting of limits on intrusion into the domestic and other environments; and the protection of private information – better known as *data protection*. [88, 151]

The right to privacy is highly protected in many countries, especially in contemporary western democracies. Yet the concept of privacy – like all legal concepts – varies in different legal systems. In the USA, privacy is considered to be a subjective right that a person can dispose of, while in Europe, privacy is merely a legal sphere that gets a special protection. According to European Convention for the Protection of Human Rights and Fundamental Freedoms, "everyone has the right to respect for his private and family life, his home and his correspondence." [135] The Constitution of Finland, Section 10 - *The right to privacy* stipulates:

"Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.

The secrecy of correspondence, telephony and other confidential communications is inviolable.

Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardize the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act." [151]

Data protection: statutes

From the thesis point of view, a central part of the right to privacy is data protection, i.e. the protection of private information. On the European Union level, data protection is extensively regulated by directives and regulations. For example, Data Protection Directive (95/46/EC) is about the protection of individuals with regard to the processing of personal data and about the free movement of such data, and Directive on Privacy and Electronic Communications (2002/58/EC) applies to the processing of personal data in connection with the provision of publicly available

electronic communications services in public communications networks in the Community. [140, 146]

On the other hand, numerous national laws include rules that affect data protection. They may stipulate more in detail and more strictly how personal information is to be handled in certain situations, or they may authorize certain usage of private information more freely than general rules would allow. Privacy is also protected by penal codes. Consequently, the legal construction of data protection rules is quite complex. The rules cannot be found in one law, but they are spread out in numerous statutes. [88, 140, 146, 149, 152]

Data protection: principles

The processing of personal data is not illegal in general. However, it should be accomplished fairly and lawfully. For example, the data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible way. The data must be accurate, adequate, relevant and not excessive in relation to the purposes for which they are collected. The personal data may be processed only if the data subject has given consent or there is another lawful basis for processing.

It is also important that disclosing by transmission, disseminating or otherwise making available to others is considered to be the processing of personal data and thus needs also consent or another lawful basis. Especially, transferring personal data outside the European Union is highly restricted. [88, 140, 146, 149]

Data protection: restrictions

There are some important restrictions to the data protection law. Usually, if a natural person in the course of a purely personal or household activity processes personal data, the data protection law is not applied. Furthermore, the data protection law applies only partially to journalistic and artistic context. [140, 149]

Processing of special categories of data

Certain sensitive information should not be processed at all without special lawful reasons. These special categories of data include racial or ethnic origin,

political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures. [140, 149]

Personal data on web pages

European Court of Justice made an important precedent in *Bodil Lindqvist* case. The court decided that it constitutes the processing of personal data, if one refers on an internet page to persons and identifies them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies. Such processing of personal data is not covered by the exceptions of the Data Protection Directive. Normally, if a natural person in the course of a purely personal or household activity processes personal data, the data protection law is not applied. However, publishing information in a web page and making personal data accessible to anyone who connects to the Internet causes that it cannot be considered purely personal activity. Thus the data protection law applies to even personal homepages of private people if they include identifiable information on other individuals. [166]

A photograph, for example, can be personal data and covered by the data protection law, if it presents an identifiable individual [168]. Therefore publishing a digital picture on a web page requires the consent of the individual in the picture or another justification from the data protection law.

Intellectual property rights

Intellectual property rights (IPR) protect intangible valuables. It is possible to own physical objects, but one cannot own nor have title to intangible objects like software, multimedia, or inventions. Those are objects of intellectual property rights: copyright, patent, trademark, etc. They can be used to prevent some unauthorized gaining of intangible objects, that is, to exclude free-riders. [33, 34]

According to GOLDSTEIN, "the principal object of intellectual property law in the United States is to ensure consumers a wide variety of information products at the lowest possible price. Intellectual property law seeks to achieve this end through the grant of private property rights enabling individuals and businesses to appropriate

themselves the value of the information they produce, thus giving them an incentive to produce still more." [37] The same principles of intellectual property rights can be found outside the USA also, although the emphasis may be slightly different. In some countries, the non-economical aspects of intellectual property rights are highlighted more.

According to LESSIG, the term *intellectual property* is a recent creation. "Before the late nineteenth century in America, the concept did not exist. Before then, copyright was a kind of monopoly. It was a state granted right to control how someone used a particular form of text. But by the late nineteenth century, so familiar was this monopoly that it was common, and unremarkable, to call it property." [70] Indeed, the roots of copyright are in prerogatives, privileges, and monopolies. There are hardly historical reasons to call the subject matter of copyright *property*. The question is whether the situation has changed. The western society has moved towards individualism. Service industry has a remarkable role in its economy. Information in all forms has become most important. Arguably, some of the most valuable objects today are intangible. Shouldn't it be possible to have property rights in them?

Property rights supply the legal framework for allocating resources and distributing wealth. [24] From that point of view it does make sense to have property rights in information. Actually, that is what the intellectual property rights are used nowadays. They do allocate information resources. Yet, it remains a policy issue, how this allocation should happen and how strong those rights need to be.

Different intellectual property rights protect different aspects of intellectual property. In general, abstract ideas, facts, knowledge, wisdom cannot be protected. More concrete ideas, that is, ideas reduced to practice may be, on certain conditions, patentable or it may be possible to claim them as trade secrets. The expression of an idea may be copyrighted. On the other hand, if the same idea is expressed in different, independent ways, each of those expressions can be a copyrighted work of its own and they do not infringe each other. The physical embodiments or the copies of copyrighted expressions can be for instance sold without assigning copyright. (See Figure 2 and Figure 3.) [41, 62, 76]

Object	Examples	Means of protection
Information	Abstract ideas, facts, knowledge, wisdom	No legal rights
	Ideas reduced to practice	Possibly patents, trade secrets, etc.
	Expression of ideas, creativity, etc.	Possibly copyright, trademarks, trade secrets, etc.
Data	Representation e.g. in binary form	No legal rights, but possibly technical protection, e.g. encryption
Physical medium	Embodiment	Possibly property rights, technical protection

Figure 2. Levels of abstraction related to intangible objects and their protection

Technical protection measures cover data, but not information, and legal rights respectively do not apply to data. In principle, an entity could technically protect any data that is in its possession. On the other hand, legal rights cover only information that lawmakers have considered worth protecting. However, legal protection does not necessarily require the physical possess of the information. That is, although technical and legal protection measures often cover same intangible objects, in principle, their coverage is quite distinct.

More information on intellectual property rights can be found – for example – in the works of GOLDSTEIN [e.g. 37], LEMLEY, MENELL, MERGES, and SAMUELSON [e.g. 69, 76] in America; BAINBRIDGE [9, 10], HUGENHOLTZ [e.g. 48, 49, 50], JACOB

et al [52], and KOKTVEDGAARD [e.g. 64] in Europe; or HAARMANN [41] and KEMPPINEN [62] especially in Finland.

Copyright

Creative works are protected by copyright. National laws, EU directives, and international treaties govern it. Anything that is original, expressed, and creative is protected by copyright. The work does not need to be registered or copyright noticed (e.g. © mark). It does not need to be artistic either. Copyright provides the right-holder with several exclusive rights. The *economic rights* include the exclusive rights to gain from the creative work, e.g. to copy, to modify, to sell, and to display the work. They can be assigned and licensed by e.g. publishing contracts or licenses. In many countries the author has also something called the *moral rights*. Depending on the country, they may include right to proclaim or disclaim authorship, and right to object any modification that would be injurious to the author's reputation. [37, 41, 52, 61, 62, 64, 69, 76]

Copyright exceptions

The strong exclusive rights, with which copyright provides the right-holders, have been tried to balance by important *exceptions*. They vary from country to country. Often they are enumerated in a copyright statute, but e.g. in the USA, they are included in *fair use* doctrine, an open limitation on copyright. Typically the exceptions include acts of reproduction by libraries, educational establishments, museums or archives and ephemeral recordings made by broadcasting organizations, illustration for teaching or research purposes, for the benefit of handicapped persons, for making current events available to the public, and for the purpose of citation or caricature. Especially, in many countries, it is legal to make copies of copyrighted works for *private use*. It is recognized by the EU Copyright Directive's catalogue of exceptions and limitations and it has been endorsed by the US Copyright Act within fair use doctrine. Nevertheless, ever strengthening IPR legislation is increasingly limiting these exceptions. For example, the anti-circumvention rules of digital rights management (DRM) legislation may in practice undercut private use exception significantly. [29, 41, 52, 64, 68, 69]

Author

The one who has created the work is called an *author*. Normally the author owns copyright originally. Often, however, the copyright is automatically assigned to the employer, if the creative work is a part of the employment. [37, 41, 52, 69]

The Anglo-American system has been stressing economic rights, promoting culture and science, and focusing on rights-owners instead of original authors. To be copyrightable, a work must be original. In France, on the other hand, *droit d'auteur* has accentuated author's personality and creativity while protecting not only the economic but also the moral rights of the author. Continental European countries Belgium, the Netherlands, Luxemburg, Spain, Portugal, and Italy, as well as countries in Latin America and Western Africa have similar copyright systems like France. Germany, Austria, and Switzerland have systems that also highlight authors' rights but their statutes furthermore strictly regulate what may be assigned and agreed. Finland and other Nordic countries have cooperated a lot when they have been developing their copyright laws. Their systems are now influenced by German strict rules, French droit d'auteur, and Anglo-American copyright laws. European Union has strived for harmonizing the copyright system in Europe. The Commission has chosen the middle road, the general continental one. The UK and Ireland as well as Germany on the other hand have had to change their laws and practices on the very basic points of copyright. [49, 53]

Several authors: joint and collective works

If a work has several authors, copyright in each separate contribution to a *collective work* is distinct from copyright in the collective work as a whole, and vests initially in the author of the contribution. On the other hand, the authors of a *joint work* are co-owners of copyright in the work. [155] A typical example of a collective work is a newspaper in which all the journalists normally have original right in their articles although they have assigned at least some of their rights to the publisher of the paper. A newspaper is thus a collection of copyrighted works that usually have different authors. A reader is typically able to distinguish between the works and the authors. However, the newspaper as a whole may also be a copyrighted work as might be, for instance, a collection of newspapers as long as the composition work

has been performed in a creative way. In a joint work, reader is not able to distinguish between the authors. A single newspaper article may be written by a couple of journalists together so that their work is indistinguishable. [41]

Non-copyrightable subject matter

One of the fundamental principles behind copyright is that copyright protection extends only to expressions and not to ideas, procedures, methods of operation, or mathematical concepts as such. [37, 41, 64, 69]

As mentioned, to qualify for copyright protection, a work must be original to the author. Especially, no one may claim originality as to facts. This is because facts do not owe their origin to an act of authorship. The distinction is one between creation and discovery: the first person to find and report a particular fact has not created the fact, but merely discovered its existence. Factual compilations, on the other hand, may possess the requisite originality. The compilation author typically chooses which facts to include, in what order to place them, and how to arrange the collected data so that readers may use them effectively. These choices as to selection and arrangement, so long as they are made independently by the compiler and entail creativity, are sufficiently original that such compilations may be protected through the copyright laws. The mere fact that a work is copyrighted does not, however, mean that every element of the work may be protected. No matter how original the format the facts themselves do not become original through association. Copyright protects only the original compilation, not the compiled facts. Like the Supreme Court of the United States noted, "this means that the copyright in a factual compilation is quite thin." [162]

| Original Idea | Derivative Idea |

Copyright

| Expression 1 | Expression 2 | Expression 3 |

| Embodiment 1.1 | Embodiment 2.1 | Embodiment 2.2 | Embodiment 3.1 |
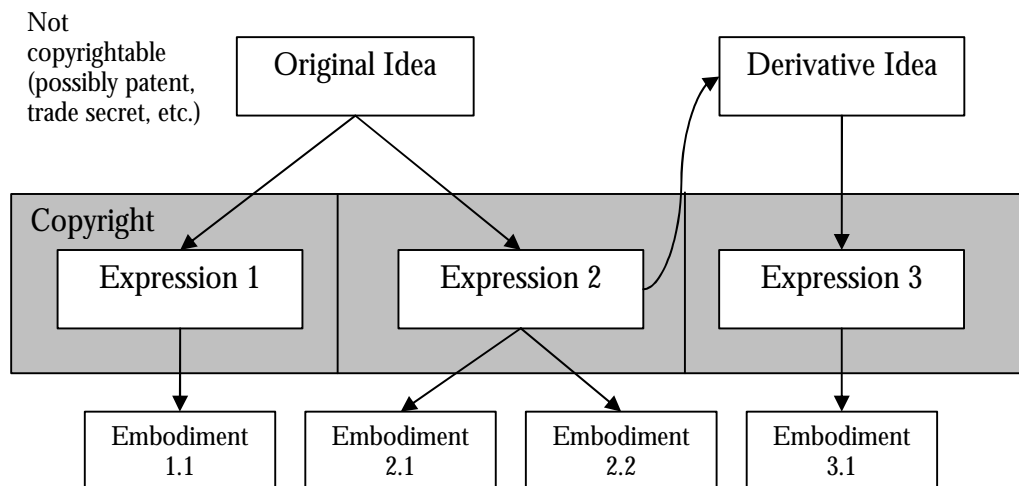
Figure 3. Intellectual property on the different levels of abstraction.

Copyright in computer programs

Computer programs form a special category of copyrightable works. They are quite different from traditional literature and arts for which copyright system has originally been developed. Therefore, national copyright laws currently include a number of special provisions on computer programs, like the limited right to make backup copies, correct errors, and reverse engineer the code. [137, 153, 155]

Database sui generis right

Databases are related to information products in many ways. More and more information is stored as data in databases. An information product can be, include, be a part of, or use a database. As a result, databases form a crucial tool in the development of the information products' market. Therefore it becomes vital important to understand what kind of rights can entities have in databases. [50, 95, 131, 141]

It is widely accepted that a database can include copyrighted works and even a database as a whole can be copyrighted if it is original enough. However, most databases are not copyrightable and their content is not copyrighted either. Yet, the

44

making of databases requires the investment of considerable human, technical and financial resources while such databases can be copied or accessed at minimal cost. Therefore some kind of protection for databases is needed. [50, 95, 141]

On the international level, World Trade Organization's (WTO) the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and World Intellectual Property Organization's (WIPO) Copyright Treaty state the fundamentals of database protection. According to Article 10 in TRIPS agreement, "Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself." [147] WIPO Copyright Treaty includes a similar article. [158]

European Union has adopted a directive concerning the legal protection of databases. It recognizes the possibility of copyrighting a database but also defines a specific *sui generis* right. [141] Several other countries are considering similar statutes. In the USA, a number of bills have been introduced in relation to database protection, but no statutes have been passed so far. [50, 62, 95, 141]

Trademark

A trademark is to distinguish goods and services to be offered for sale, or otherwise purveyed in business, from those of others. The main purpose of a trademark is to guarantee a product's genuineness. Trademarks are typically names, phrases and logos, but any kind of mark that can be represented graphically and by means of which goods marketed in business can be distinguished from those of others may be a trademark. A trademark is the legal protection of a brand. [36]

Contents / The Whole	not original	Original
no substantial investments	No legal protection	The whole is not legally protected, but copyrighted contents
a substantial investment	Database *Sui Generis* Right	*Sui Generis* Right + copyrighted contents
Original	Copyrighted as a whole	Copyrighted both as a whole and contents

Figure 4. Copyright and the Sui Generis Right in a database.

Patents

A patent gives an exclusive right to exploit an invention commercially. More precisely, it gives the patent-holder a right to forbid others from using the invention. In principle, patents are granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application. An invention can be a product or a process that provides a new way of doing something, or offers a new technical solution to a problem. The invention cannot be commercially made, used, distributed or sold without the patent owner's consent. Patent is limited to a specific period of time – usually for a maximum of around 17 to 20 years – and to a certain territory – usually to a country. [11, 37, 76]

The patent system is supposed to promote inventions and industrial advances. Arguably, patents provide incentives to individuals by offering them recognition and material reward for their inventions. These incentives should encourage innovation.

It is however questionable, how well the patent system actually achieves that goal. Currently, it is valuable for especially large companies to have an extensive patent portfolio that can be traded with other companies. On the other hand, smaller companies are often required to apply for patents because many venture capitalists and potential acquirers believe that patents as such add value to a company. Patents are also often used as a marketing and brand-building tool to give a high-tech impression of a company. Do any of these motivations to apply for a patent really require the patent to be issued? Actually, for many companies, it is enough to file an application. A pending patent already brings all the benefits the company is seeking. It seems that the lawmakers' idea of issued patents protecting certain useful technological inventions is giving way to a number of other ways to benefit from the patent system.

International treaties harmonize national patent laws worldwide, although some differences exist. Most of the dissimilarities are only formal and do not affect patenting in practice. For example, in the USA a patentable invention must be novel, useful, and nonobvious while in Europe an invention should be new, involve an inventive step and be susceptible of industrial application. [69, 114, 121, 136, 156] Nevertheless, sometimes disparities in development may lead to incompatibilities between jurisdictions. In practice, national patent authorities consider the patentability of an invention separately. At the end of the day, the same invention can be found patentable in some countries and not patentable in the others.

Non-patentable subject matter

Patent protects information on a higher level of abstraction than for example copyright (see Figure 2 above). In general, a patent protects an idea reduced to practice. That is, it does not protect totally abstract ideas nor only new implementations or expressions of ideas. It does not protect mere data or investments either. [11, 37, 76]

Patent application

Patents do not appear automatically; they have to be applied for. It is actually quite a laborious and expensive process to get a patent. A patent application normally

contains the title of the invention and an indication of the technical field. It also includes the background and a description of the invention, in a way that others could use or reproduce the invention. Drawings and other visualizations often help to describe the invention. The application also contains various claims that determine the extent of protection granted by the patent. [11, 135]

Patent litigation

The patent rights can be enforced in a court, which holds the authority to stop patent infringement and award damages to the patent owner. On the other hand, a court can also declare a patent invalid if a third party has successfully challenged it. A patent infringement suit in a court can be expensive. Also, in addition to remarkable costs, the threat that the patent is declared invalid on one side and the threat that the infringing activity is stopped on the other side and the overall uncertainty of the litigation output make most companies reluctant to patent litigation. Therefore the threat of trial is often enough to force the parties to negotiate and cases are frequently settled outside the courts. Noteworthy, most patents are never litigated.

According to ALLISON et al, ninety-nine percent of patent owners never even bother to file suit to enforce their rights. So why do they apply for patents at all? ALLISON et al have listed from the literature several suggestions: [7]

- The patent owners may simply be irrational.
- Many valuable patents can be overlooked by their owners.
- Many of these patents are being licensed without the patent owner ever needing to go to court.
- The existence of the patents themselves is a sort of signaling device to consumers, competitors, venture capitalists or other investors.
- Patents are a sort of trading card that companies need in order to protect themselves from other companies with patents.
- The patent system is a giant lottery, with a patent the equivalent of a lottery ticket: unlikely to pay off, but very valuable if it does.

ALLISON et al compared the characteristics of litigated patents to those of issued patents generally, and found important differences in a range of dimensions. They based their study on US patents – it is unlikely that their results are directly applicable to patents in other regimes. However, my own experience mainly from Finnish IT companies suggests that usually they do not apply for patents to get exclusive rights in certain technologies, but mostly to improve their image in the eyes of investors and customers, and to get chips for the rough game that is played in the marketplace.

Patentable inventions

To be patentable, the invention must be *novel,* i.e. new. In other words, there needs to be some new characteristic which is not known in the body of existing knowledge in its technical field. This body of existing knowledge is called *prior art.* The invention must also show an *inventive step.* Finally, the subject matter must be patentable under law. In many countries, discoveries, scientific theories, mathematical methods, aesthetic creations, plant or animal varieties, discoveries of natural substances, schemes, rules, methods for performing mental acts, playing games or doing business, and methods for medical treatment are not patentable. [11, 37, 76]

Right in portraits

Right to one's own picture is an ambiguous topic, on which most countries do not have a specific statute. Germany is the most noticeable exception. Since the scandal of pictures on dead Bismarck, Germany has had a law against taking and publishing a person's image without the person's consent. It includes an important exception: pictures on public figures can be taken and published without consent as long as the public figures are outside their private spheres, like homes. [72, 148]

In Finland, the central provisions on right to own picture are in the Penal Code. Chapter 24 criminalizes offences against privacy, public peace and personal reputation. Section 6 – Illicit observation – determines, where it is lawful to take pictures, and Section 8 – Invasion of personal reputation – states, what kinds of pictures can be legally distributed. [60, 152]

Section 6:

"A person who unlawfully watches or monitors with a technical device

(1) a person in domestic premises, a toilet, a dressing room or another comparable place, or

(2) a person in a building, apartment or fenced yard that is closed to the public […], where this violates the person's privacy, shall be sentenced for illicit observation to a fine or to imprisonment for at most one year.

An attempt is punishable."

Section 8:

"A person who unlawfully

(1) through the use of the mass media, or

(2) in another manner publicly

spreads information, an insinuation or an image of the private life of another person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for an invasion of personal reputation to a fine or to imprisonment for at most two years.

(2) The spreading of information, an insinuation or an image of the private life of a person in politics, business, public office or public position, or in a comparable position, does not constitute an invasion of personal reputation, if it may affect the evaluation of that person's activities in the position in question and if it is necessary for purposes of dealing with a matter with importance to society."

In other countries, rules are more or less similar: it is acceptable to take decent pictures in public places and publish them, but the pictures may not invade personal reputation. On the international level, this can be derived from Article 12 of UN's

Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." [60, 154]

Copyright to a picture belongs to the photographer, but even the copyright law may acknowledge some rights to one's own picture. According to the Finnish Copyright Act, Section 27, in the case of a portrait executed on commission, the author may not exercise his right without the permission of the person who commissioned it or, if that person is deceased, that of the surviving spouse and heirs. Also, in accordance with Section 40 c, the party commissioning a portrait to be made by photographic means has the right, even if the photographer has reserved the right to the work for himself, to authorize the inclusion of the portrait in a newspaper, periodical or a biographical work, except where the photographer has separately reserved the right to prohibit such inclusion. [153]

The strengthening data protection law discussed above hands individuals more powerful tools to prevent the publication of pictures on them than the vague right to one's own pictures has been. Photographic images, if identifying an individual, are construed as personal data under the data protection law in Europe. This means that even if the picture is taken in a public place and does not invade personal reputation, it may not be published, e.g. in a web page, without the consent of the person it represents except in journalistic or artistic context.

Contracts

Contract is an agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law. Often the term 'contract' also refers to a document, the writing that sets forth such an agreement. The fundamental characteristic of a legal agreement is its *bindingness*: the contract binds the parties. Contracts are the primary legal means to manage rights in information products within bilateral relationships. If two entities know each other and are willing to commit to certain terms and conditions, according to contracting freedom, they are free to agree on issues extensively. On the other hand, however, contracts do not bind outsiders: contracting parties cannot in general give obligations to third parties.

Where two entities conclude a contract, they generally enter into a two-way obligation - one undertakes to provide the other with goods or a service and the other undertakes to pay the price. Each of the parties to the contract is also bound by an obligation towards the other to compensate if the contract is not performed properly or not performed at all. Especially on computer networks, it may sometimes be difficult to identify the contracting parties and be sure what the terms and conditions are. The mandatory laws can limit the contracting freedom furthermore. Therefore, the contracts do not always bind the contracting parties either. Instead, laws are required to define the legal framework to control issues that are not governed by contracts. [36, 176]

In many cases, contracts can extend legal rights. For example, copyright law provides right's owner with certain statutory rights. However, within the context of a contractual relation, the parties can agree that they have more rights than defined by the law. Say, according to a contract, an author might have a right to proclaim authorship or a publisher could restrict redistribution even if the legal system did not ensure it. [48]

The term *commitment* refers to something that an entity agrees to accomplish in the future. A written contract and an oral agreement are possible ways to manifest commitments. [36, 65] Yet, it is also possible to send another entity a message expressing a commitment, either a conditional commitment, like an offer, or an unconditional commitment like an acceptance notification or a promise.

For example, an e-book distributor can send an end-user a message telling that the end-user is allowed to use the e-book on the condition that the end-user pays a certain price and accepts certain other terms. This message does not constitute an agreement because it does not bind the end-user until the end-user accepts the conditions stated in the message. It is rather an offer. However, if the offer binds the distributor, it expresses distributor's commitments. The distributor is committed to grant the end-user a license to use the e-book on certain conditions. The end-user in turn can send the distributor a message telling that the end-user accepts the terms and will pay the price. This message represents the commitments of the end-user.

After the end-user has accepted the distributor's offer, there exists an agreement between the end-user and the distributor even though it is not manifested in a one contract but in two or even in several commitment notifications.
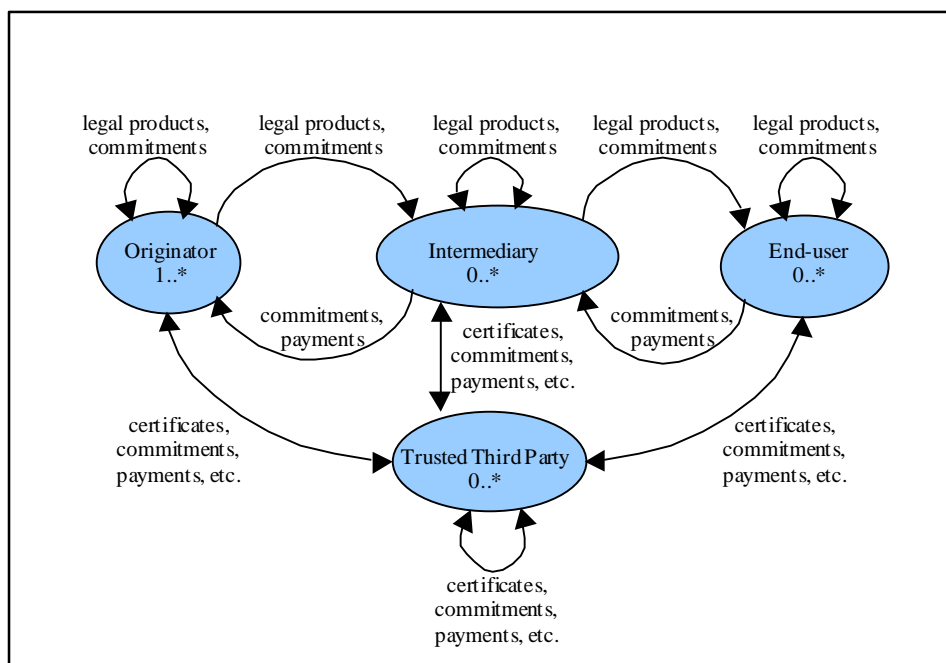
Figure 5. A sample legal process of e-book transactions.

In Figure 5, originators have created, invented, collected, or otherwise brought about contents in legally significant ways. Intermediaries, including agents, publishers, service providers, operators, retailers, etc., add new components, new value and new rights into the legal products and forward the combinations further. End-users of e-books get licenses to use e-books. They send payments to intermediaries that share them with other parties. Transactions are secured using cryptographic methods and trusted third parties. The term commitment in the figure refers to commitment notifications that entities send to each other. The notations 0..* and 1..* refer to cardinalities. In general, there should be one or more originators and any number of intermediaries, end-users, and trusted third parties. If there are no intermediaries, originators transact directly with end-users. In the undesired situation that there are no end-users, the process of course is reduced to meaningless. If the parties trust in each other enough, there do not need to be any trusted third parties.

A loop arrow going from an actor to the same actor means that if there is more than one actor of that kind they can communicate with each other.

Labor law

Labor law refers mainly to the rules and principles that govern relationships between the employees who work in return for pay under the authority and direction of employers. It covers also relations between employees' representative organizations (labor unions) and employers or their organizations, as well as relations between any of these and the government.

Tax law

Tax law is the area of legal study that deals with taxation. [36]

Administrative law

Administrative law refers to the rules and principles that govern the organization and operation of the executive branch of government and the relations of the executive with the legislature, the judiciary, and the public. [36]

Liability, torts, and damages, esp. products liability

Legal *liability* means that somebody is legally obligated or accountable. It refers to legal responsibility to another or to society. Legal liability is enforceable by civil remedy or criminal punishment. [36]

Tort is a civil wrong, relating to private rights – as distinct from a *crime* – for which a remedy may be obtained usually in the form of damages. It is a breach of a duty that the law imposes on everyone in the same relation to one another as those involved in a given transaction. It is the legal, non-contractual basis for compensation. There is a non-contractual obligation where a person who is responsible for loss sustained by another person is required to compensate the victim, in cases not linked to the performance of a contract. [36, 176]

Damages refer to money that is claimed by, or ordered to be paid to an entity as compensation for loss or injury. They are the sum of money which a person wronged is entitled to receive from the wrongdoer as compensation for the wrong. In a

contractual relationship, the aggrieved party is usually entitled to damages for loss caused by the other party's non-performance which is not excused. [36, 176]

Products liability means that the producer or the manufacturer is liable for damage caused by a defect in a product. Furthermore, anyone who imports a product for distribution in the course of business is also responsible as a producer. Even a supplier or a seller of the product can sometimes be liable. The injured person must be able to prove the damage, the defect and the causal relationship between defect and damage. A product is defective when it does not provide the safety which a person is entitled to expect. In Europe Union, products liability is usually applicable only to damages to private people, not to businesses or organizations, while in the USA, it applies to any buyer, user, or bystander who is injured in person or in property by a defective product. In Europe, the damages cannot exceed the actual losses. In the USA, it is possible, although rare, that additional punitive damages are awarded to punish the manufacturer or seller that has acted with recklessness, malice, or deceit. [36, 92, 119, 120, 139]

In general, products liability is quite strict. A producer cannot usually avoid liability by agreements, disclaimer notices, or other juridical tricks. The best way for a producer to secure against products liability claims is to produce as high quality products as possible.

Marketing law, consumer protection, competition law

Several legal areas regulate business actions in the market place. *Consumer protection law* protects individuals against unfair trade and credit practices. It does not ensure just the safety of goods and services, but also those economic and legal interests that will enable consumers to shop with confidence. *Regulation of marketing* governs the methods that an entity may use while marketing its products and services to customers. *Competition and anti-trust law* is the body of law designed to protect trade and commerce from restraints, monopolies, and price-fixing. The general objective of the antitrust law is to maintain competition. Companies may try to achieve as powerful position in the marketplace as they can, but it is illegal to misuse a dominant position. [36, 176]

METHODS

<div style="border: 1px solid">

Wiio's Laws about Predicting the Future

1. *We tend to overestimate the near future.*

2. *We tend to underestimate the far future.*

3. *We tend to believe that technology changes the basic human nature.*

- Osmo A. Wiio [80]

</div>

This thesis covers many areas. I am discussing on technological, legal, economic, and other societal issues. Therefore, the thesis is necessarily somewhat interdisciplinary or multidisciplinary and I have needed to use several methods to accomplish this work. In many areas I have heavily relied on literature and large parts of the thesis are thus based on observations from other scholars' publications. Nevertheless, the main contributions of the thesis are the legal analysis of the set of scenarios and the model to analyze *legal challenges related to the future information products and services business models.*

Some discussion is required to explain, how I came up with the list of the future legal challenges and analyzed them. At first sight, it seems that legal challenges should be analyzed using the methods of legal science. However, the question is about forthcoming issues while legal science mostly uses court cases, statutes, and their preparatory works as its sources and derives theories by analyzing them. Thus it is

hardly possible to tell anything much about the future using conventional jurisprudential methods.

Instead, futures research provides us with more suitable methods. Especially scenarios are useful when I want to describe how the world will be like and what kinds of legal challenges may occur. Scenarios used in other fields of science are typically quite broad. In this thesis, scenarios are relatively narrow: they merely describe a possible service or a use-case that is grounded on literature, existing services, and discussions with content providers, operators, vendors, and other actors. [14, 74]

I do not claim that any of those scenarios would actually come true. Neither is their actual probability of being realized in the focus of this thesis. Instead, they are to form a picture of possibilities and concerns that may exist in the future. Methodically, they must be believable and concise possibilities. The non-linearity of actual change is therefore not a focal issue. I endeavor to answer, what would happen in given conditions, i.e. in presumed situation. Scientifically I am facing serious concerns since I am speculating without immediate possibility to refutation. I believe, however, that it is possible to test the validity of the scenarios later with true use cases or prototypes further derived from the scenarios. [22, 44, 74]

On the other hand, it can also be argued that the question is not so much about validity as *relevance* of the research. Indeed, from an interpretivist/critical perspective it is not possible to create an accurate model of reality in the first place. Instead, the reality is interpreted and reinterpreted in various social contexts, aiming at exposing relevant aspects and viewpoints of the reality for a particular discourse in a particular context. Therefore, instead of formal validity, what matters is the pragmatic and operational relevance of the results to the stakeholders and the context. [20, 128]

The major problem I faced was how to create scenarios that cover relevant, possible situations adequately. If I had created them randomly, I would not have been able to claim that they embody important issues sufficiently. To avoid such biasing, I had to be able to create the scenarios in some systematic way. Also, using a systematic method helped me to diminish the effect of my own values and beliefs.

Certainly, the scenarios reflect my personal views, but the approach I used reduces that bias and makes it visible to the reader to estimate it.

I have constructed a method to study future legal challenges. I have derived the following requirements of the method from the above defined scope and research questions:

- The method must bring out *legal challenges*. It should enable a person with legal education to point out the legal areas in which critical challenges are.
- The method must bring out legal challenges of *commercial entities*. It may be applicable to non-commercial entities also, but that is not relevant in this thesis.
- The method must bring out legal challenges of commercial entities that provide *information products and services*.
- The method must bring out *future* legal challenges. The time span defined above is about two to ten years.
- The method must bring out legal challenges of entities that provide *consumers* with products and services. The main emphasis is on B2C markets, as discussed above.
- The method must bring out legal challenges that are relevant for *strategic product and business planning and development*.
- The method should bring out legal challenges especially in relation to the *Internet* and *mobile* networks.

My approach is based on factors and their attributes. I need to understand the main factors that have effects on legal challenges. To see how the factors will develop in the future, I studied their attributes.

I think that specific factors and their attributes can be identified that by interacting with the existing law imply the legal challenges. The factors that I am focusing on are *technological* and *socio-economical*. When the existing law is applied to them, the legal challenges will arise. By legal challenges I mean difficulties in legal reasoning or somehow unsatisfying outcome of the legal process. I summarize from literature, which attributes of each factor mostly seem to relate to future information businesses. Then I create scenarios so that each of those attributes occurs at least in

one scenario. Next, I identify legal challenges involved in scenarios. I also check the attribute list to identify legal challenges directly from them. The legal challenges are then classified by legal areas and analyzed.

I am calling attributes also phenomena that in futures research are usually called for example weak signals and trends. From the perspective of the thesis, however, it is not necessary to distinguish those concepts. It is sufficient to mention that they are all issues that have notable effects on the dynamics of the factors.

The method has some noteworthy threats to validity:

- First, I may have made mistakes in the definition of the factors that mostly affect legal challenges.

- Second, I may choose wrong attributes to characterize the dynamics of factors.

- Third, even if the factors and attributes are correct, I may have created scenarios that do not represent adequately the future situations. I may even make erroneous conclusions based on otherwise well defined scenarios because I am not able to test and verify them.

- Fourth, I may identify legal challenges incorrectly or insufficiently.

- Fifth, I may analyze the issues erroneously.

Based on the careful design of the study, however, I am quite confident that these threats are limited. Moreover, I have been able to check that the scenarios are reasonable by discussing them with our industrial partners and other experts.

The method has been criticized, because I have first created the scenarios and then analyzed them myself, which could cause some bias. To avoid it, I have additionally borrowed scenarios that others have created (namely MC2, Between, and ISTAG scenarios, see Chapter Scenarios below) and analyzed them also. The problem with those other scenarios is that I do not know exactly how well they have been created, what kind of processes have produced them, and what presumptions have been made. Basically they have been created for other purposes and there is no guarantee that they suit for my study. Yet, I have tried to select scenarios that seem to have been created properly and that probably have similar enough presumptions.

Therefore, combining my own scenarios and the borrowed scenarios I believe I have been able to avoid bias that analyzing my own scenarios might have caused, and yet I have had reasonable control on at least some of the scenarios. The fact that my own scenarios and the borrowed scenarios introduced similar legal challenges make me confident that the chosen approach is acceptable.

The legal analyses of the scenarios are my own. Also, in Legal Implications, besides the literature survey, I introduce some deductions of my own. I have accomplished those using jurisprudential methods.

I have carried out the legal analysis of the scenarios using a similar method that a practicing lawyer would use, if a client asks to assess what kind of legal problems there might be in a given case. Of course, the lawyer would use the knowledge that the legal education and prior experience have provided, but also systematically go through different legal areas and check specific issues in each of them. From the methodological perspective, this kind of analysis might be described as hermeneutical – or maybe heuristic.

After I have created the list of legal challenges, I have listed the major distinguishers that cause those challenges in businesses. Then I have discussed the implications of those challenges and distinguishers.

EXAMPLES OF INFORMATION BUSINESSES

DIGITAL PICTURES

Digital technologies are changing the world of photography dramatically. The replacement of film by a digital sensor, processing capability, and memory in the camera has reached enormous popularity within both professional photographers and hobbyists. Digital camera sales worldwide was about $24 billion in 2004 and rise 29 percent to reach $31 billion in 2009. Digital camera sales are expected to nearly replace film camera sales by 2008. The top five worldwide market leaders in digital camera sales in 2004 are Canon, Sony, Olympus, Kodak, and Fuji Photo Film. [180]

Another, probably at least partly a distinctive phenomenon, is the camera phone: a mobile phone that includes a digital camera. It provides users with capabilities to take pictures with a device that people are almost always carrying with them, and immediately send the pictures to other people using the mobile device's communication functionalities like multimedia messages (MMS). According to InfoTrends Research Group, the worldwide unit sales of camera phones have gone up from 150 million in 2004 to 370 million in 2005. Camera phone sales are expected to experience a remarkable growth to reach 847 million units in 2009. In 2004, rapid adoption of camera phones worldwide generated an additional 29 billion digital images captured. [180]

One of the most interesting features of digital pictures is that they are easy to share with other people. Attractive new products and services are being created to support these activities. Metadata will be a key enabler to help users to find images

and to manage them. For example, PhotosToFriends, former MobShare, is a mobile phone picture sharing system developed by HIIT and Futurice. With the help of metadata, it enables immediate, controlled, and organized sharing of mobile pictures, and the browsing, combining, and discussion of the shared pictures. [115, 186]

ELECTRONIC BOOKS AND NEWSPAPERS

The thing that's been around for thousands of years and is so powerful is the word. The power of the word is extraordinary, and if the word is embodied as text, that, too, is powerful, regardless of whether the text lives as ink on pulp or signal on flat-panel display. Words aren't going away, and I think the book/no-book argument is dumb once you realize that all we're talking about are variations in display technology. I'm not anti-book or anti-print; it's just that soon we're going to be doing our "printing" in a different medium.

- Nicholas Negroponte [13]

ELECTRONIC BOOKS

E-books as information products include not only the contents but also metadata, i.e. information about the contents, and possibly computer programs that are parceled up. It is possible that some parts of an information product are distributed separately to the end-user. For example, parts of metadata like a key to decrypt the contents may be delivered by a trusted third party while an intermediary distributes the rest of the product. Yet all those parts form a logical whole and they can be called a product.

E-books enable a vast amount of new business possibilities. There are few ways to sell a traditional printed book. In general, it forms a single transaction to sell a

book: a seller gives a book to a customer and the customer gives payment to the seller. However, in addition to the traditional single-transaction mechanism, there is an unlimited number of other ways to sell an e-book. For example, an e-book can be given for free for awhile and charged later if the customer wants to keep it. Or a customer can be charged based on the usage: he or she will pay per read page, for instance. This will not only enable better price discrimination but also creates a valuable continuous relationship between an e-book provider and a user. [118]

These new business models, however, rise up questions that are both legal and technical. An e-book publisher should be able to control and enforce its intellectual property rights to get payments. The legal projection of an e-book is a legal product; it may include several legal components. Therefore the publisher should also be able to take care of the rights in components and share the revenues accordingly. [125]

E-books will be distributed through networks that may be wireless. There can be a number of different kinds of intermediaries between authors, publishers, sellers, and customers. For instance, network operators and service providers will have an important role. It is essential to have secure mechanisms to perform the business transactions. The technology will be based on cryptographic methods and trusted third parties. Therefore there will be a number of important actors involved in these transactions. All of them need to be able to communicate with each other using well-defined protocols and languages. Communication between entities includes e-books, but also commitment notifications, payments, certificates, and so on.

NEWSPAPERS

As ENLUND points out, newspaper production actually consists of two very different production processes linked together. First, there is the creative process of putting together the newspaper pages with their mixed contents of editorial matter and advertisements – the manufacturing of an original. Next, a high volume mass production and distribution of copies follows this. These two types of production are fundamentally different. (See Figure 6 below.) [31]

The digital technology will dramatically change especially the latter. If newspapers are delivered in electronic form through networks, no more printing is needed and the distribution of copies can be completely automated. However, the creative process may not change that much. New technology will probably somewhat change the way journalists work, but the same human creativity remains behind the editorial work.
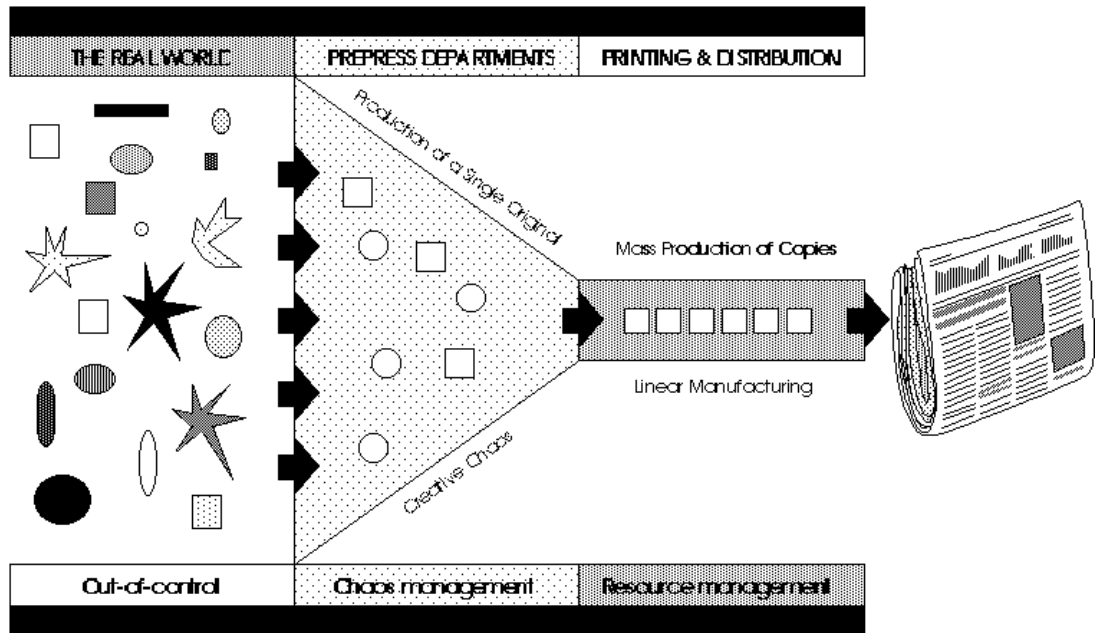
Figure 6. The different processes of newspaper production according to ENLUND.

HETEMÄKI and OBERSTEINER have forecasted that US newsprint consumption is more likely to decline than increase. [46] Conventional printing and distribution will probably decrease. By 2010 economic incentives and marketing benefits will lead to that many newspapers are published only in digital form. In 2020 most newspapers in the USA and in several other countries are published in workdays exclusively in digital form. It will not pay to print papers any longer. Lately, information technology has increased paper consumption. Information technology and paper products have been complementary companions. In the long run, nevertheless, they will become rivals and information technology will eventually win. [32, 45]

MUSIC

Music industry is probably the best known field of digital rights management. That is because of the widely reported court cases of Napster and other peer-to-peer music distribution systems. However, digital rights management in music products is much more than just a couple of questionable court cases. In the following I give a brief overview of the field.

COPYRIGHT IN MUSIC

Considering copyright in music, composers and lyricists are normally the original copyright owners. The arrangement can be a derivative work and its creator owns copyright in it. However, the rights in performances and recordings are also interesting. The performance and the recording as such are usually not considered copyrighted works. Instead many countries, like for instance Finland, provide rights for them through legal doctrines called neighboring rights. [41, 153] In the USA, common law has provided some protection to performances, but copyright law has not. However, in 1994, pursuant to the GATT TRIPs Agreement, federal neighboring rights to protect live musical performances were enacted. [11, 147, 155] According to GATT TRIPs Agreement, member countries provide performers with right to prevent the fixation of their unfixed performance and the reproduction of such fixation. Performers have also the possibility of preventing the broadcasting by wireless means and the communication to the public of their live performance. Producers of phonograms have the right to authorize or prohibit the direct or indirect reproduction of their phonograms. Broadcasting organizations have the right to prohibit the fixation, the reproduction of fixations, and the rebroadcasting by wireless means of broadcasts, as well as the communication to the public of television broadcasts of the same. [147]

Intellectual property owners can authorize special organizations to license their intellectual property. A user would pay a license fee to such an organization to obtain rights to the intellectual property. The organization then accounts the payments to

the owners of the intellectual property. These kinds of organizations are quite common in the music industry, though they exist in other fields of intellectual property also.

The American Society of Composers, Authors and Publishers (ASCAP) is a membership association of over 80,000 American composers, songwriters, lyricists and music publishers. In Japan, an organization called JASRAC is authorized to govern the rights of lyric writers, composers and music publishers. For example, in Germany, Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA), in France, Société des Auteurs, Compositeurs et Editeurs de Musique (SACEM), in the United Kingdom, The Performing Right Society (PRS) and Mechanical Copyright Protection Society (MCPS), and in Finland, Teosto protect the rights of their members by licensing and paying royalties for using copyrighted works.

The organizations mentioned above are national. Music distribution on the Internet does not obey boarders. A user may download music from whichever country through the Internet. Therefore national organizations are facing serious challenges. Perhaps they are able to network so that those national organizations together can form an international system. Another possibility is to establish a new international organization that could operate worldwide.

PEER-TO-PEER SOLUTIONS

In general, copyright owners have an exclusive right to copy their works. That is, making copies of a copyrighted work without permission infringes copyright. However, in most countries, it is legal for private persons to make few copies for their own use. In the USA, for example, this right is within the statutory *fair use,* while some other countries like Finland have a special private use provision in their copyright law. [41, 69, 76, 153, 155]

An essential prerequisite of making copies for private use is that the number of copies is small. It is legal to make a photocopy or two of a book, but not to print hundreds of copies in a printing press.

Napster was an Internet company that provided software for sharing information on the Internet. Napster's software made it easy to share and copy music files over the Internet. Users allowed others to download files directly from their computers. Napster had a database that included reference information about the available files so that users were easily able to find the files they wanted anywhere in the world. Although Napster did not keep any of the music files on its own servers, it effectively helped users to download their favorite music to their computers. Napster became enormously popular and the number of files downloaded using the software was very large. This is why RIAA, the Recording Industry Association of America filed a lawsuit against Napster. RIAA did not want to sue individual users although they were actually copying the music files in large quantities. The law suit ended Napster in its original form. [183, 187]

There are many alternatives following Napster, Gnutella, KaZaa, Morpheus, WinMX, IMesh, BearShare, LimeWire, and AudioGalaxy being some of the best known of them. Therefore even though Napster was shut down, other solutions keep distributing music files all over the Internet. Those newer services are more distributed and decentralized. Therefore, they are less vulnerable to lawsuits and harder to control.

Peer-to-peer networks are not fundamentally illegal. It is perfectly possible to use them in a legal way. The problem is that the current technologies make it too easy to infringe copyright and thus they label the whole peer-to-peer networking illegal. Still in the research phase, there exist interesting alternatives that enable music sharing in a legal way, respecting legal rights and license terms. DiMaS is a good example of peer-to-peer systems for multimedia producing communities to publish their works on P2P networks. It enables producers to insert content metadata, to manage their rights in works, and to charge for the content consumption. [107]

FACTORS TO SCENARIOS

SOCIO-ECONOMIC VIEWPOINTS

SCARCE INFORMATION

What makes information valuable? First of all, to be economically valuable the information must be somehow *scarce*. The concept of scarceness includes that a commodity is both limited and needed. Exclusive rights in information no one wants are worth little. Information can be limited for several reasons: it might be due to the costs of production, reproduction, or transaction. Figure 7 elucidates how different factors affect scarcity.

The production of information, that is bringing certain information into existence, can be costly for many reasons. For example, information may be about a new idea that is hard to invent. Or it can be difficult to express the idea in a way that it fulfills the demand of the potential users. Or, it can be laborious to build a new collection of existing information: in terms of the database sui generis right, the obtaining, verification or presentation of the information may require substantial investments.

Production → Reproduction → Transaction → Users

Factors of production
- Ideas
- Innovations
- Knowledge
- Skills
- Creativity
- Labor

Factors of reproduction
- Material
- Labor
- Capital

Transaction costs
- Search costs
- Negotiating costs
- Other specific investments (e.g. relationship specific investments)
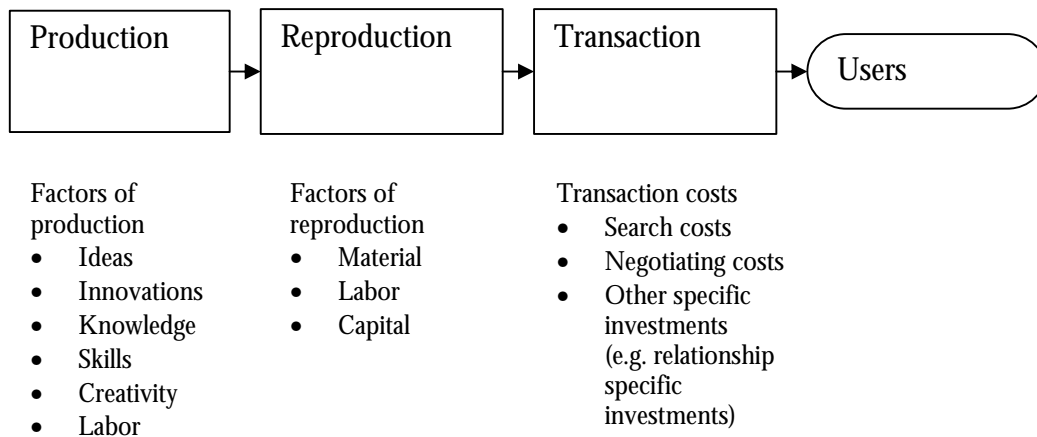
Figure 7. Sources of scarcity related to information products.

As examples, let us consider a couple of different information products that can be valuable. First, after a hard research work that also demands a lot of knowledge an engineer comes up with a new idea about a better way to manufacture a certain appliance. Information about that innovation is demanded, because companies that produce those appliances can save money and improve the quality of their products by using the innovation. At the first place, only the inventor, the engineer, knows about the invention, which makes the information scarce for the others. The information is therefore valuable.

The second example is a textbook about a method to manufacture a certain appliance. The writer has not invented that method. In fact the method is already fully described in a scientific article that is publicly available, but the article is quite theoretical and hard to understand. The writer of the textbook explains the method clearly and carefully. After reading the book, a professional can easily use the method. In this case, some information about the method is freely available, but the free information does not fulfill the demand. Instead the better expression of the same ideas is more demanded. If the textbook is not freely available, it is a scarce resource of information and thus valuable.

The third example is a collection of descriptions of known methods to manufacture a certain appliance. If there is a large number of those methods, collecting their descriptions may be difficult even though nothing new is invented or expressed. The large amount of work needed to obtain the information, to verify it is correct, and to present it properly makes the information scarce.

The modern information technology has made the reproduction or copying of information goods inexpensive. Especially, information in digital form can be copied with low costs. Usually only a little material, labor, and capital is needed to reproduce information. However, from customers' viewpoint, reproduction can be costly if it is restricted by technical or legal protection. For example, to make an unauthorized copy of an information product that is protected by a technical protection system may require a lot of work and expensive apparatus. On the other hand, making an illegal copy of an information product that is legally protected poses the risk of severe reimbursement. Therefore unauthorized reproduction is not necessarily as inexpensive as it may seem and the means of protection can be used to manage the scarcity and the value of information.

The other way to analyze the value of information is to examine the demand side. Several factors have effect on the demand. SHAPIRO and VARIAN [118] as well as MESSERSCHMITT and SZYPERSKI [78] have published excellent dissections.

One of the most important factors on the demand side is *network effect*. The more users an information product has, the more appealing it is for new users. The other important factor is *lock-in effect*. After somebody has started to use an information product it can be expensive to replace that product with another. [26, 78, 118]

Transaction costs include search costs, negotiating costs, and other specific investments. They may have significant effect on the total costs of acquiring an information product. Digital rights management can affect transaction costs. DRM technical tools can, for example, enable a permanent connection between a service provider and a user. This can make it easier to find information products from the same provider and automate the negotiating process thus decreasing the search and

negotiating costs. On the other hand, the same tools can also be used to increase transaction costs if a user is willing to procure services from another service provider: rights management tools can strengthen the lock-in effect.

GENERAL VALUE CHAIN

According to TIMMERS, a business model is an architecture for product, service, and information flows, including a description of the various business actors and their roles; and a description of the potential benefits for various business actors; and a description of the sources revenues. Also, according to Timmers, a systematic approach to identifying architectures for business models can be based on value-chain deconstruction and reconstruction – that is, identifying value chain elements – and identifying possible ways of integrating information along the value chain. [127]

To add value and to deliver information products to end-users, entities need working business models and value chains. However, the suitable business models may be quite different for various information products. For instance, the music industry and the publishing industry have traditionally used quite different models.

In figure 8, a sample general value chain is illustrated. Note that infrastructure providers are not shown. For example, operators that merely provide access to communication networks seem to be sinking into the infrastructure. Their income will probably be more and more based on fixed fees – e.g. monthly service fees – and they are not able to charge for each information product they transmit. Their business models are based on effective production and economies of scale while an actor in a key position along the value chain may charge a remarkable share of the price of each product.

The figure shows a number of actors. In general it is hard to build that long a value chain that is also profitable. At least, transaction costs rise too much. Instead, an actual business model is usually based on few actors. Computer networks and electronic delivery can be used to reduce links in the chain. Each of the actors in a chain includes several links. For example, a publisher can also be an editor, an

aggregator, and a filterer. It is important for an actor to understand its business model and position in a value chain.
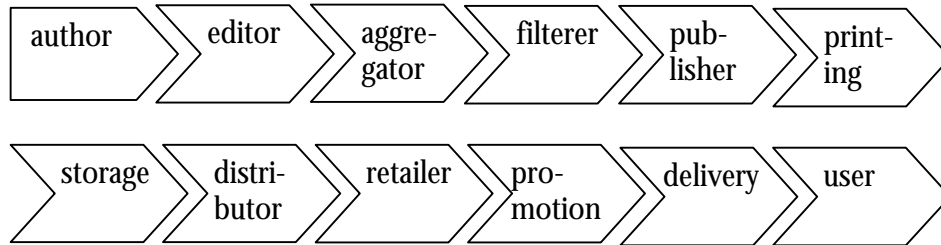
Figure 8. A sample value chain related to digital information product.

It is customary nowadays to speak about value networks instead of value chains. This emphasizes the increasingly complex and dynamic nature of value constellation. However, in practice, a network usually projects into a chain when a single product or service is delivered. That is, the concept of network underlines the number of possibilities how an information good can be delivered while the chain illustrates the actual route through which a certain good travels from the originator towards the end-user.

ECONOMIC TRENDS

The fast pace of technological progress makes people often forget that the laws of economics do not change easily. [118] Yet, economic attributes do not alone determine the future, but they have a crucial role in the reality where financial and other organizational decisions are made to selectively support different technologies. Therefore, I try to map the key economic attributes. The first three of them describe entities and the rest three describe their economic environment. [96]

The *dynamic capabilities* of the entity will become more important. In firms, this will mean strong change culture through specialized scope and focus on innovative niche products and markets. Second, the *resources* will become more *intangible*. Rights

in them are limited and fuzzy and therefore call into attention new methods for intellectual asset management. Intangibles may be turned into value not only through traditional income from licensing and sales but also from strategic positioning. Entities will use more efficient licensing strategies based on detailed product differentiation. Third, organizational entities and internal processes will become more integrated with *low hierarchy*. This change can be described as a shift from vertical bureaucracies to flexible horizontal entities. The lifetime of a low hierarchy may be short as new kinds of ad-hoc hierarchies emerge for specific purposes. [96, 118]

On the environment level, mainly on the markets, *network economics* and network effects will perhaps be the most determinant attributes. Firms will tie alliances, partnerships and joint ventures for strong external relations. Products and services that rely on demand side economies of scale will turn out to be the winning ones.

Second, *lock-in* has become a key term in describing information economy. Most profitable products are those that can be turned into long-term services. Lock-in situations will be increasingly self-feeding since as the other party knows more of the other, the information exchange can be further tailored according to the needs of the parties.

Third, the networked economy strengthens the importance of *branding*. For many new products and services it will be crucial to get public attention and recognition among users. Holder of a strong brand may also franchise or license it to enable growth in new markets. Brands break ground in the society at large; brand marketing is getting closer to culture and culture to marketing. Sports, music and movies are already commodified into brands. On the other hand, existing brands do not automatically guarantee success on the digital environment. [96]

The industrial age, very much an age of atoms, gave us the concept of mass production, with the economies that come from manufacturing with uniform and repetitious methods in any one given space and time. The information age, the age of computers, showed us the same economies of scale, but with less regard for space and time. The manufacturing of bits could happen anywhere, at any time, and, for example, move among the stock markets of New York, London, and Tokyo as if they were three adjacent machine tools.

- Nicholas Negroponte [84]

This thesis intends to analyze legal challenges related to future information businesses. Legal and regulation issues are always related to the society. It is not possible to study them without trying to understand what kind of society they are associated. Therefore I am briefly illustrating the world around the future Mobile Internet.

It is arguable if our society — or any society — should be called an *information society*. Information has always played important role in every society. Some characteristics, however, of the modern society suggest that information is a more essential part of it than it used to be. CASTELLS, on the other hand, calls the modern society a *network society* emphasizing how networks change the world. [18, 19] Information is the fundamental part of a network society. According to CASTELLS, "the network society is a social structure made of information networks powered by the information technologies characteristic of the information paradigm." [18]

One of the special characteristics of the modern society is the fact that entities are increasingly dependent on information as a central strategic resource in industrial and economic development. It has a significant impact on their competitiveness. All technological changes have depended on information, but now both the input and

the output of business processes can be pure information or as CASTELLS points out, "what is specific to the informational mode of development is the action of knowledge upon knowledge itself as the main source of productivity." [19] The economy turns towards information extremely rapidly. This trend allows closer links between regional, national and international economies. Also, it breaks down the conventional barriers between financial sectors, as all work, including manufacturing, becomes increasingly a matter of the transmission of information. [189]

The rapid rise of transnational corporations would have been impossible without global information networks. Currently, there are hardly more than a couple of dozen national economies bigger than the economies of the major corporations. The networks facilitate the *globalization* and it depends on them heavily. While networks permit economic decision-making on a world scale in real time the term globalization does not refer simply to improved ease of communication and interaction between nation states, nor is it purely limited to the economic and business spheres. [19, 189]

Globalization refers also to significant cultural changes, including for example greater migration, more international tourism, the development of "world music", greater international co-operation in political, economic and ecological matters. CASTELLS also indicates that there is "a trend that we would call 'bureaucratrization' in the Weberian sense that is the predominance of the rationality of means over the rationality of goals." [19, 189]

The *aging* of population and the changing demographics have both positive and negative effects on society. Older people may provide companies with business opportunities and pensioners can have a positive impact on culture and society at large. On the other hand, especially the worsening dependency ratio introduces severe challenges to the whole society.

At the level of individuals, *the changing concept of work* is affecting daily life. Concepts like *networkers* and *flextimers* [19] or *e-lancers* [73] reflect that change. Flexibility in the working arrangements is bringing about new work-life policies that allow employees to have more control on their jobs and personal life. Also some

traditional work environments will change: more virtual offices will emerge, more employees will telecommute, and non-traditional work schedules will be the norm. [19] Described by HIMANEN, a hacker ethic contests what was before the basis of individuals' "protestant" duty to work. In some sense the hacker ethic is a counterforce to the market culture. Hackers enter into information creation and exchange motivated by enthusiasm, joy and passion, not just money. [47]

Information technology may introduce severe *challenges to political* systems. According to CASTELLS, the collapse of Soviet Union was largely due to the incapability of assimilating informationalism. [17] HIMANEN illustrates the role of information technology in the Kosovo crisis of 1999. [47] Several countries are currently trying to limit their citizen's access to the Internet for political reasons. Mobile technologies make the future even more challenging for a political system based on people's limited access to information.

As information technology affects people's lives in many ways there can be significant changes in their *minds and behavior.* At worst this can appear as an addiction but there are many other possible phenomena also. It will be seen how people react on increasing telecommuting and virtual working communities. Restructured social identities can affect how people feel about themselves. The ever increasing surveillance and ubiquitous computing change people's notion on privacy. In general, there are lots of important issues on the individual level yet to be researched.

The reduction in the constraints of space is also an important part of the modern society. The actual geographical locations will be largely irrelevant in an economy, which has passed, in NEGROPONTE's terms, from shifting around atoms to shifting around bits. [84, 189] Yet, it is interesting to realize how much the geographical location still means on the personal level. For a human being, the tangible world is nevertheless important.

TECHNOLOGICAL ADVANCES

INTRODUCTION

This thesis is about legal challenges and rights management in relation to the future information technology and networks. To find out what will those future computers and networks look like, it is necessary to try to draw a picture on the future. There, technologies have an important role as enablers. However, it should be noted that technologies do not determine the future; they just enable many kinds of different futures. Completely other factors determine which one of those possible futures will actually come true. On the other hand, those other factors, like economy and society at large, also affect technological development. Like ROSENBERG has shown, technological change does not occur inside a black box, but in close interaction with the other fields of society [108].

It should be also noted that technological development is not so much about significant, separate inventions, but continuous evolution. Although it is typical in public to pay attention to certain heroic individuals or remarkable technical inventions that seem to have had significant impact on a certain technology, it would usually be more adequate to see them as a part of on-going evolution [12]. Adapting from DAVID, technological development is a path dependent process that is not ergodic or random; it is unable to shake free of its history [26]. Therefore, though I am presenting in the following some specific technologies or even inventions, they are just to represent the technological development. I am not trying to describe any technology in detail. Merely, I am attempting to give an overview picture on what kind of technologies affect this area.

LAYER MODELS

It is often useful to illustrate computer communication using layer models. For example, OSI reference model is divided into seven layers, and the Internet TCP/IP

model is also layered. On the bottom of those models, below the first layer, is the physical medium, like cable. Above the layers are applications that send and receive messages. Each layer takes care of some important part of communication. Figure 9 below summarizes the two common models. It is not necessary to go into details of these models. From this theses point of view, however, layered models are helpful to clarify that the Internet is very different on different layers or viewpoints. The layers hide their technical details from each other. For example, in principle, higher layers do not need to know what the physical medium is, because the lowermost layer hides it from the others. Therefore upper layers do not need to change their behavior even if the physical medium is changed. On the other hand, the lower layers do not need to care what applications are using the network connection, because the upper layers hide that information.

Let us consider an example. If a user wants to browse certain web pages, the browser software sends a request to the web server in HTTP protocol. This protocol is on the higher layer of TCP/IP model as shown in the figure. The protocols on the lower layers take care of the actual data transfer. Therefore neither the browser nor the web server needs to care about the physical medium. The fact that the user may have an Ethernet or a modem connection through the wired network to the server or a mobile terminal device that accesses the Internet using GSM network is hidden from HTTP protocol, the web server, and the browser. Mobility, in this case, does not require any changes on the higher levels of the model. As a matter of fact, it seems that in most cases, the mobility can be hidden on the lower layers and it does not need to affect services.

On the other hand, some services themselves change their behavior depending on the mobility of users. For example, an office application, like a word processor or a calendar, might provide an end-user with different kind of services depending on whether the user is sitting behind a desk and using a powerful computer with broadband network access or whether the user is hiking on a mountain carrying only a small mobile device and having only a slow wireless network access. A weather service application could behave differently depending on user's location and the weather data available on that area. Also, the mobility may have, for example, legal

implications that force service developers build their services so that they are legal also when users are moving. For example, if a user moves from one country to another, the service should keep track that it complies with territorial laws and agreements all the time.

OSI model	Internet TCP/IP model
Layer 7: Application layer	Application protocols
Layer 6: Presentation layer	Telnet, FTP, SMTP, HTTP, SNMP,
Layer 5: Session layer	etc.
Layer 4: Transport layer	TCP / UDP
Layer 3: Network layer	IP
Layer 2: Data Link layer	IEEE 802.3, ATM, Frame Relay, etc
Layer 1: Physical layer	
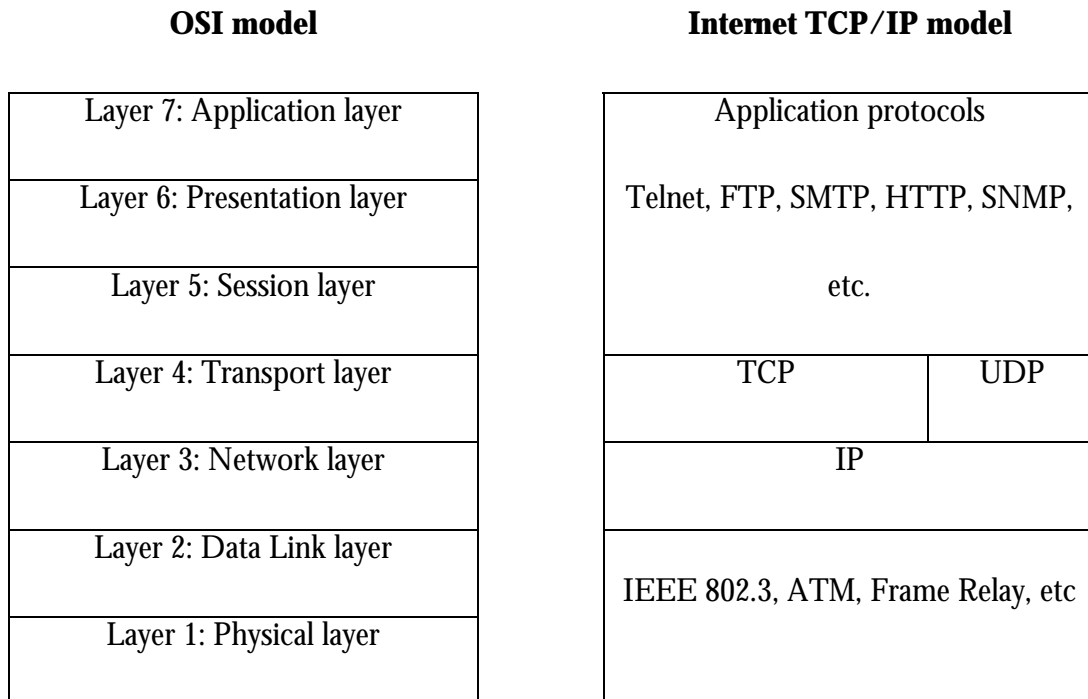
Figure 9. OSI model and Internet TCP/IP model compared according to KARILA *[182]*

MOBILE NETWORK

The Mobile Internet is the future computer network to which the end-users connect largely using mobile, wireless appliances. It should be emphasized that the concept is not well defined. Both the terms *mobile* and the *Internet* are ambiguous. Therefore I do not try to draw strict borders around the Mobile Internet, but I merely describe essential characteristics of the concept to name the research domain.

The meaning of mobility depends on whether we see the Internet through a service level or an underlying protocol level. On the protocol level, a significant property of mobility is that the access point is not fixed. The point in which a

terminal logically accesses the Internet varies. Therefore packet routing to a mobile terminal on the protocol level needs to be dynamic and it may change during the communication. Obviously, challenges to protocols, routing mechanisms, and naming conventions are remarkable. This viewpoint does not necessarily imply that the terminal should be wireless or portable.

On the service level, however, the word mobile refers to users' ability to move around while using the Internet. The term *nomadic*, on the other hand, sometimes refers to users' ability to connect to the Internet in different places, but not necessarily move while they use the Internet. For example, a laptop computer that is connected to the Internet using a modem, a cord, and a telephone line is a nomadic device. A nomadic device does not need to be wireless. Instead, mobile end-user terminal devices in practice must be wireless and portable. The focus in this thesis, digital rights management on the Mobile Internet, is mainly related to the service level. Therefore, I emphasize the wireless and portable properties of terminal devices. Some of the issues however will refer also to the protocol levels.

The network itself and many end-user devices will remain wired. In the foreseeable future, wireless bandwidth will not achieve the orders of magnitude that are already available with wired connections. Therefore, the backbone network as well as all those connections that need large capacities will not be wireless. Instead, wireless connections will be common where the large bandwidth is not essential and where end-users benefit from the ability to carry network devices with them while they move.

The *Internet* is a computer network system that combines many smaller networks. It is the global network of networks. It is based on a common addressing system and communications protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). The Internet is very large connecting hundreds of millions of computers and users around the world. There are many ways to define what the Internet is. Some technical definitions provide an unambiguous and clear description, which nonetheless are not suitable for our purposes. For example, I cannot leave some networks, appliances, and services out of this study just because

they are based on, say, some exceptional communications protocol. From the rights management point of view, it is necessary to concentrate on how users, service providers, and other high-level actors realize the Internet, and pay less attention to the technical details.

From this thesis' point of view, there are some important attributes that describe the Internet.

First, there are several widely used services on the Internet. Especially, the World Wide Web (WWW), electronic mail, and file transfer and sharing mechanisms seem to be popular today. It is hard to call for example a computer an Internet device, if one cannot access most of the public WWW pages, e-mail system, and at least some file transfer possibilities using that computer. Therefore I consider an access to those services an essential part of the Internet.

Second, the Internet services are usually more or less interactive. In order for something to be called the Internet, it needs to be possible for the user to be able to interact with the services. Also, the Internet is a computer network, which means that the computers communicate with each other online. They are usually simultaneously connected to the Internet. It is however quite typical that, for example due to some technical error, a terminal device is temporarily unconnected. Many computers are nowadays connected to the Internet using modems that are not always on. On the Mobile Internet for a long time there will be geographical areas that are not covered by wireless networks. If a user travels through such an area, the terminal device will not be connected to the Internet there. Therefore, even if a terminal device is switched on and the user wants to access some service on the Internet, the connection is not always possible. I still want to call that sort of device an Internet terminal device. A continuous online access is not a criterion for the Internet. Yet an Internet device should have online access to the Internet services often enough and preferably it should have some features to support offline usage of the Internet services, like drafting e-mail messages without connection.

On the Mobile Internet, the user switches between access points and is often even disconnected. However, the illusion of continuous service should be

maintained. This requires new infrastructural properties on the network. When the user is online, these properties should help to deliver the best possible quality of service adapted in accordance with the user's profile and the physical context. The network would try to predict which services the user is going to request next. While the user is offline, these properties would manage the user-information and make it available for the proper services and for them only. If we for example travel from San Jose, California to Helsinki, Finland, the network would prepare for the evident data replication at Helsinki airport by pushing the user-information into a nearby server in Helsinki.

Third, the Internet is quite an *open* network. Open means that the Internet specifications and standards are publicly available so that anyone can build new hardware, software, and services to be used on the Internet. Also, it means that the Internet is publicly available. Not everybody has possibilities to buy the necessary devices and an access to the Internet, and some countries or jurisdictions have severe restrictions to the usage of the Internet. Still, in general, the Internet is largely available, and it is not required to be for example a member of a certain organization to get the access.

OPEN, SEMI-OPEN, AND CLOSED NETWORKS

It is an essential property of the Internet that the network is open. As discussed above, both the standards and specifications of an open network as well as the network itself are publicly available. A *closed* network in this context, for the sake of comparison, is a network that does not allow its users to connect services outside the network. For instance, an organization's local area network (LAN) that is not connected to the Internet at all is closed. It merely provides connections to the other machines and services in the same network.
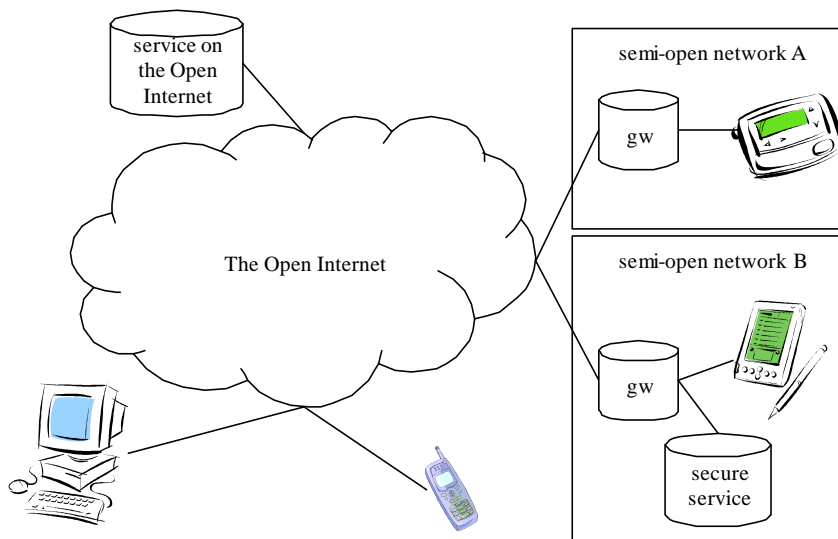
Figure 10. The structure of the open and semi-open Mobile Internet.

Interestingly, there are lots of networks that fall between these two extremes. They are not completely open or closed. Instead, they do provide an access to the services on the Internet, but this access is more or less limited. For example, a user may access only certain services on the Internet. Figure 10 illustrates the overall structure of the Mobile Internet. Often these kinds of semi-open networks are connected to the Internet using some kind of a gateway (*gw*) that allows certain traffic but prevents the other. For example the world's leading Internet access provider America Online, Inc. (AOL) used to be quite closed a network. Yet, it has been opened gradually and today it would be difficult to claim that AOL is not a part of the Internet. [169] In the Mobile Internet, appliances like WAP phones [192] and I-mode phones [179] offer a limited access to the Internet based on the access providers' policies. Therefore WAP and I-mode networks are typically semi-open networks and in my opinion they provide mobile Internet access.

On the other hand, a truly open network is also accessible from outside. A semi-open network, even if it allows its users to freely access the other networks, typically restricts other users' access to its services from outside.

Although open networks are usually desirable, a closed or a semi-open network can offer important advantages. It does not need to use all the standard protocols

and tools that often lack important properties like security. Instead, a proprietary protocol, for example, can provide a much higher-level confidentiality, data integrity, and authentication. Closed networks can also offer more sophisticated methods for traffic accounting and invoicing as an example. There will probably exist lots of closed and semi-open networks on the edge of the Internet in the future also.

It should be mentioned that terms open, semi-open, and closed could have different meanings in other contexts. For example depending on the viewpoint, the same network can appear as an open, semi-open, or even closed network. A terminal manufacturer, a network operator, and an end-user may have quite different opinions on whether the network is open or not. In this thesis, I once again emphasize end-users' point of view because the digital rights management questions seem to be most likely to appear on that level.
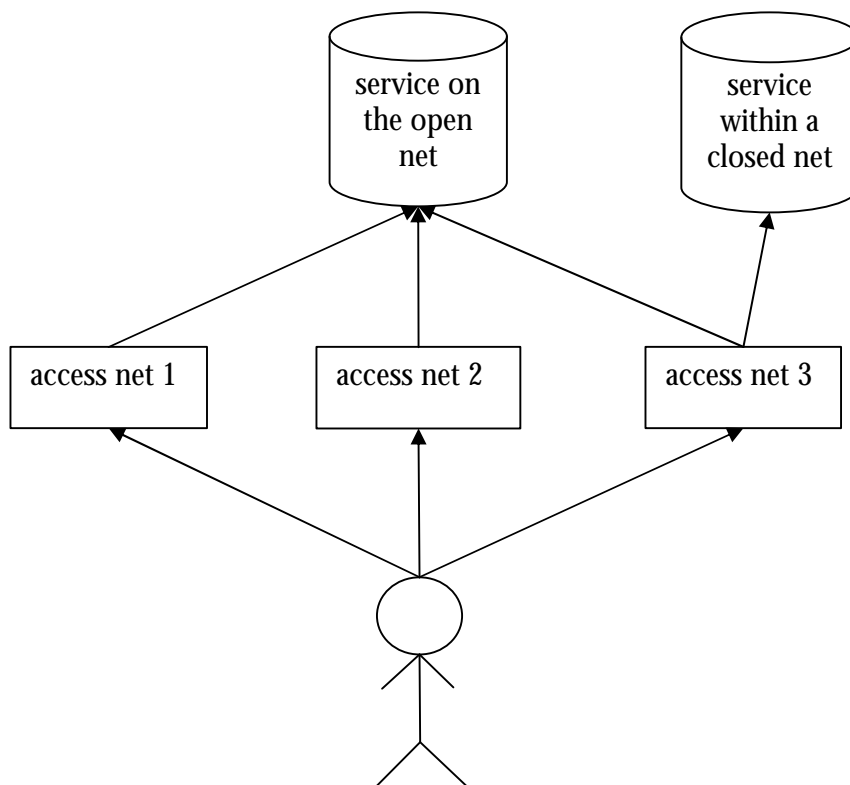
Figure 11. Services through different access devices and networks

Figure 11 illustrates how some services on the open Internet are accessible through many kinds of open and closed networks and using many kinds of terminal devices. On the other hand, some services are available only on a certain closed network that provides for example adequate security and accounting capabilities.

APPLICATION SERVICE PROVIDER AND PEER-TO-PEER MODELS

At the early phases of information technology, computers were big mainframes. Users accessed them using terminals, which did not have any processing capabilities. All the processing was conducted in central mainframes. Because all the data was stored and processed in a central computer, management issues were typically not very serious. For example, documents were stored in a central archive, they were easy to find, and there were hardly any confusion about versions and access permissions. Programs were easier to develop, because they were generally to work in one environment only. Also, it was rather simple to change or upgrade programs, because the changes were needed to make in only one place. The problems started to emerge after the invention of personal computers. They enabled data processing on every desktop. The programs and data were spread everywhere. After that the management of data integrity, program and document versions, access rights, and so on became a nightmare. Each personal computer formed somewhat different computing environment from all the other computers, which make software development as well as maintenance more difficult. Without central management it was hard to find data, keep track of versions, and so on.

The development of the *client/server* model attempted to combine the best parts of centralized and decentralized data processing. Users access data flexibly through their client workstations, but the data is actually stored and managed in a central server. Clients and servers are typically located in different computers that communicate through networks. Software is divided in two parts: client programs that are executed in workstations and server programs executed in servers. Client programs typically offer user interfaces and some processing capabilities while server programs are invisible to users and they carry out most of the processing and provide

storage services. The decision what a client should do and what is left to a server is basically a matter of performance. The network between the server and the clients introduces some delays and its capacity may be quite limited. It often makes sense to accomplish those operations in a client that need to response rapidly to users actions. On the other hand, client programs are normally not easier to develop and maintain than personal computer programs in general.

A natural evolution from the client/server model is the *application service provider* (ASP) model. While networks become more efficient it is possible to move more and more on the server side without compromising system's performance. In the ASP model everything but the basic user interface is initially located in a server. For example, normal office applications such as calendars, e-mail, and word processing, can be provided as services. Users do not need to install any applications. They only need a computer with adequate network capabilities and a browser program. If some specific programs are needed in the client computer, they are loaded dynamically from the server while the service is used. This is much less demanding for a computer. Therefore more inexpensive hardware could be used as client machines. ASP services are expected to become an important alternative, not only for smaller companies with low budgets for information technology, but also for larger companies as a form of outsourcing and for many services for individuals as well [191]. Ultimately, however, ASP companies could largely replace the shrink-wrap software product industry.

Peer-to-peer or *P2P* is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access data and resources in one another's computers. Users can for example share files or spare computer cycles, which makes network a huge distributed computer. P2P technologies include peer group collaboration, distributed content sharing, peer group file sharing, peer resource discovery, and peer access and control. [4, 21, 63, 191]

The best known P2P file-sharing applications have became enormously popular. The dominating P2P file sharing networks may have millions of simultaneous users

sharing hundreds of millions of files. In addition to file-sharing, other applications, such as P2P computing, i.e. sharing processing resources on a network, are becoming increasingly popular.

According to KILMER, "P2P applications can be one-to-one (1to1), where the client owner accesses client information or capability from a distance (wired or wireless); one-to-many (1toM), where some specific group can access a service available within a client; or many-to-many (MtoM), where anyone can access the client. The most common P2P application, content sharing falls into the MtoM category, and will not translate well to wireless until third-generation networks can provide sufficient bandwidth." [63] In its pure form, P2P networks do not have servers and clients, but the user terminals or the edge devices act as more or less equal peers.

ASP model will probably be quite important on the Mobile Internet. Mobile devices will not have storage capacity and computing power to run locally all the software and services that the users will need. Therefore it will be important to divide applications so that only the minimal part of it is in a terminal device and the rest is kept in servers on the network. On the other hand, P2P model is gaining increasing popularity. As suggested below, we will probably see combinations of these two models: basic information and resources will be shared in a P2P fashion, but some value added services will be provided in accordance with ASP model.

SUPERDISTRIBUTION

Packaging information in secure containers enables a concept called *superdistribution*. It is one special form of peer-to-peer distribution: others can make copies and even repackage information products and further distribute them, possibly profiting from the repackaging, while respecting the rights of the owners of the original content. A user can for example give copies of an information product to friends telling them that it is a good product and recommending the acquaintances to use it also. A user can even package several products in a secure container with user's

own set of rules for access. Importantly, those rules depend on the rules specified by each of the individual information products that remain enclosed in their own containers. That is, the user cannot give others more rights than the rights holder of an individual product has permitted. The user then recommends the information products to acquaintances and sends copies of the package to them. [126, 188]

Many of the acquaintances are willing to buy the package because someone they trust recommends it. The one who buys the package must obtain all the necessary rights, including the rights to the collection, and the rights to any of the individual information products. Superdistribution therefore makes distribution more effective and enables a chain of value-adding activities, while respecting the rights and restrictions imposed by all the content owners. [126]

According to SCHULL, information products can be copyright-protected, so that while for-pay content may be formatted in such a way that it is not easily pirated, freely browseable preview content can remain accessible and inviting to its recipient. Superdistribution works, and it proves that the sale and marketing of digital goods is fundamentally different from that of e.g. conventional print products. Content producers should not focus on preventing copying. They should encourage redistribution. [188]

IDENTIFICATIONS

To solve many of the questions risen up in this thesis, it is viable to be able to identify objects. That is, entities, persons, devices, and information products should have unique identifiers.

Information products can be identified by assigning a persistent identifier. There have been several attempts to standardize such identifiers. They include Digital Object Identifier (DOI), Persistent URL (PURL), and Uniform Resource Name (URN). For example, DOI has two components, known as the prefix and the suffix. These are separated by a forward slash. The two components together form the DOI. For example, *10.100X/123456* would be a valid DOI, where *10.100X* is the

prefix and *123456* is the suffix. The prefix is a number or a string that is assigned to an organization that wishes to register DOIs. An organization then again may register any number of prefixes. For example, a publisher may have only one prefix or it could have a different prefix for each publication series. Each suffix, on the other hand, is unique to a given prefix and it identifies the digital object, like an information product. The suffix can be any alphanumeric string. This can simply be a sequential number, or it can make use of an existing identifier, like an ISBN code. For example, ISBN-90-411-9785-0 would be a valid suffix. The combination of a prefix for an organization and a unique suffix provided by the organization itself avoids any necessity for the centralized allocation of DOIs. [174, 185, 190]

In principle, a DOI can apply to any form of intellectual property in any digital environment. It seems that this will largely solve the identification problem with respect to information products. However, some difficult semantic questions remain unsolved. For instance, if an information product is adapted or it has a number of versions, each of them should be identifiable, but DOI does not give any specific support to versioning. A DOI can be assigned to products with numerous versions, but it is up to the publishers to determine to what level of granularity and to which versions DOIs will be assigned to a work. The semantics of versioning is left to the entities that use DOIs. Moreover, usually only the publisher controls the semantics and thus, if other entities use different semantics, it can be difficult to apply DOIs in certain situation. If entities, say, have different notions of versioning and DOIs are based on one notion; other entities have troubles in applying the DOIs to their versioning scheme.

For devices, unique identifiers are even more difficult to define since there are so many different technologies available. Some of them already include identifiers. For example, GSM mobile phones have identifiers on several levels: each phone has an identifier, smart cards or SIM cards that store for instance user information have identifiers, and there are identifiers for user accounts, like account number and telephone number. However, none of those identifiers is universal. That is, other technologies, like PDAs or PC computers use different identifiers.

The identification of human individuals seems to be the most difficult one. It is difficult to reliably relate any physical identification to a human being. However, that is a small problem compared to legal and ethical issues related to privacy, anonymity, and identity. In general, everybody should be able to remain anonymous and to keep privacy. On the other hand, a human being may act in a large number of roles. A person at work, at home, at leisure activities, and so on has many roles that should be distinguished. For example, usage rights like private use or fair use are often different depending on the role and a license may only cover certain role-based usages. Therefore it is hardly possible to build solutions that in general rely on human beings direct identifications. Instead, most systems need to depend on indirect user identification based on for example device identification. [e.g. 85]

There are also many other objects that should be identifiable. For example it would be useful to be able to identify some context factors, like the country where the user is currently located. At the moment, it is often possible to identify some of those factors, but not unfailingly and precisely in all the cases.

DIGITAL RIGHTS MANAGEMENT

One of the most controversial topics in the field of this thesis is digital rights management, *DRM*. People are vigorously arguing whether strong intellectual property rights and digital rights management are good or bad. The content industry, music companies, movie producers, and book publishers among them, claim that proper means to protect intellectual property are essential to the cultural development. Intellectual property law is to allow individuals and businesses to benefit from the value of the information they produce. It gives them an incentive to produce still more. Rights are vital to create revenues for authors. Without reasonable compensation writers, composers, artists, and other creative people will not produce as many works for others to benefit as they could.

On the other hand, the active movement emphasizing the freedom of information has a negative attitude towards legal rights that restrict the use of

information. One of the most noticeable characters of the movement is professor LAWRENCE LESSIG. He declares that it is not question about whether the authors get paid, but who controls the revenue flows. The authors would get their compensations even if there did not exist any intellectual property rights. Instead the laws protect media companies that are not flexible enough to survive otherwise in the new digital environment. [71]

It makes the situation more controversial that in many fields of the content industry ownership is highly concentrated. The large corporations own the majority of the publishers and rights holders of the industry. In general, the concentration of control of rights and revenue flows is problematic.

The fundamental function of a legal system is to enable adequate protection for the entities within its jurisdiction. Should, however, a legal system protect existing companies and create artificial entry-barriers for new-comers, or should it let the markets decide who the winner is? Should it especially support for example those who create content, those who make it available, or those who use it? The big question is how to find the right balance.

Intellectual property rights have been developed in a quite different world than the digital environment that is rapidly emerging. Many rights protect something that was valuable yesterday, but does not have that much significance any more. For example, according to SCHULL, copy protection does not make sense any longer, because copying and distributing copies are essential to business in the digital content industry. Instead, legal systems should support new business models based on inventions like superdistribution: people should be encouraged to copy and further distribute information products. The question is how to make sure that the content creators and providers get adequate compensation or other incentives to produce new valuable information products. [188]

Digital rights management systems can also extend intellectual property rights far beyond what is provided by the legal system. For example, exceptions that restrict intellectual property rights because of – for example – fair use, private use, criticism, comment, news reporting, or teaching are generally believed to be useful. However,

using powerful rights management systems, rights-holders can pre-empt those exceptions and significantly enlarge their rights. Also, it is widely accepted that no-one should have exclusive rights in certain information, especially in facts. Nobody can own the laws of nature, for example. Rights management systems enable nonetheless control over facts also. Lawmakers are currently extending the legal protection of the technical protection tools so that circumventing technical means becomes widely illegal. Although facts are still not directly protected by laws, they get strong indirect protection if they are stored in a system that is legally protected. This development is most concerning. [145, 147]

From technological point of view, there is an important question to make. It is hardly possible to develop a fully tamper-proof rights management system. For that reason, does it make any sense to use rights management systems at all? It is not possible to make a fully burglar-proof house either, but people are still using locks in their doors. Oftentimes, it does make sense to employ reasonable means of protection although they are not perfect. Even a technical protection system that has evident limitations may be sufficient to prevent most unwanted usages. For a rational, capable, potential infringer, the question is that of cost/benefit: does the cost to circumvent the protection overcome the benefit of getting the information? For a less rational potential infringer, it is often the question of ability and bother: one is not capable or does not want to take the trouble to bypass the protection. Moral and psychological issues should not be ignored either. For many of us, the fact that something is protected means that it is not allowed to be accessed and that as such is a reason not to circumvent the protection but to respect the right holder's will whether legally grounded or not.

The best known example of problems related to digital rights management has been the original Napster file sharing service. Millions of users shared music files without paying anything to music companies. After legal fights, the music industry succeeded in killing Napster. The unauthorized copying of music files did not however stop. Napster was replaced by a number of new services that are more distributed, more de-centralized, and more difficult to control. Since Napster case, several other trials against file sharing services have been initiated, but it seems that

not all the services can be shut down by court orders. By destroying Napster, the music industry may have lost a "good enemy" that could have been controlled unlike some of its follow-ups.

Until recently, the free peer-to-peer music sharing services have been virtually only way to get music from the Net. Some interesting commercial substitutes have appeared – today the most interesting being Apple's iTunes and new commercial Napster 2.0. The commercial services do provide an important alternative and they can kill the arguments that music sharing for free is necessary because there are no services subject to a charge. However, their success remains to be seen. [170, 183]

In this thesis, I present some facts and opinions about the usefulness of digital rights management, but the underlying assumption however is that it depends on the situation and on the entities whether DRM is needed or not and what kind of DRM should be used. I do not endorse strong legal rights and their strict enforcement nor do I claim that no legal rights should ever be applied to information products. Also, I do not claim that technological solutions alone could solve all the problems that information technology has caused. Nor do I believe in the omnipotence of any legal constructs.

Rights management is performed with the help of different kinds of technical tools. In the following I am briefly presenting some of them.

A key enabler of DRM is *cryptography*. Cryptographic algorithms are used to encrypt information in a way that unauthorized usage of that information is not possible – or at least, it is difficult.

Rights expression languages (REL) are meant to describe rights so that all the entities involved can act in accordance with them. A rights expression language provides a means of expressing use and access rights to digital assets. For example, using a REL, an entity could describe that it gives to another entity a non-exclusive license to complete specific operations on particular information certain times in a specified period of time if the other entity complies with certain conditions like pays certain fees. Such information is adequately included in the rights description part of

an information product's metadata. It is not necessarily packaged with the actual content, but it may be delivered, for instance, in a separate certificate. [39]

On the other hand, rights expression languages can also be used to specify that an information product can be used for free on certain conditions, "only some rights reserved", or even that the product can be used freely and the rights holder has no claims, "no rights reserved". Interesting undertakings related to open source ideology are trying to implement this in practice – most notably *Creative Commons* project. [173]

A rights expression language is a central component in a digital rights management (DRM) system. A DRM system is intended to protect information and allow its usage in accordance with associated contract terms and conditions. The contract is written in a REL that is formal and machine-interpretable. Often, it is desirable that a computerized DRM system is able to enforce the contract. On the other hand, even if the contract is not totally enforceable by computers, it can still be used, for example, when searching for information that can be used in a certain way.

In principle, a contractual relationship between two entities cannot be comprehensively interpreted by a computer system. Ultimately, a human being, namely a judge, is needed to interpret the legal content of a contract. On the other hand, the automatic making and interpreting of contracts could – not only enable automatic enforcement by DRM systems – but significantly speed up business processes and reduce transaction costs. Therefore, it will be interesting to see how largely contracting can be automated and on which level computers will be able to interpret contracts.

In the future, DRM systems will be essential tools to enable the distribution of information products both for business, private (e.g. sharing user-created content within a community), and public (e.g. public health-care or libraries) purposes. Therefore it is vital to develop RELs that are expressive enough to represent the various models of distributing information products. Yet, to be usable in practice, a REL should not be too broad, but focus on rights expressions that are important.

It is quite demanding to define a formal language that can be used to correctly express all the necessary rights in different jurisdictions. There is some interesting work going on to define such a language. Especially, eXtensible rights Markup Language (XrML), currently better known as MPEG-21/5, and Open Digital Rights Language (ODRL) are quite promising attempts [25, 38, 39, 184, 193].

XrML - eXtensible rights Markup Language, formerly known as Digital Property Rights Language (DPRL), recently also called as MPEG-21/5, is an interesting work towards developing tools for digital rights management. The language was first created in 1990's at Xerox Palo Alto Research Center (PARC). The further development is now carried out by ContentGuard, Inc. XrML can be used to specify rights for digital works. It provides a mechanism in which different terms and conditions related to access, fee, and time can be specified and enforced for the different operations on digital documents such as view, print, and copy.

XrML is especially interesting because there are several excellent scholars, e.g. MARC STEFIK, at Xerox PARC, who are well aware of intellectual property right issues and who have contributed to the development of XrML. ContentGuard is trying to get XrML into the position of the industry standard. In August 1999, Adobe and Xerox announced a strategic initiative to integrate Adobe's PDF technology with Xerox ContentGuard rights management solution. [172, 184, 193]

XrML seems to be quite mature and well-defined rights description language. On the other hand, ContentGuard has strict license terms and there are several patents that are claimed to cover not only XrML, but also other rights description languages. Therefore, licensing and other legal issues related to XrML leave serious questions.

The example in Figure 12 adapted from XrML Specification 1.3 [193] gives an idea how the usage rights can be described in XrML. It tells that John Doe is allowed to view a particular book ("A book of James") in certain period of time using a specific device.

```
<?xml version="1.0"?>
<!DOCTYPE XrML SYSTEM "xrml.dtd">
<XrML>
    <BODY type = "WORK" version="2.0">
        <WORK>
            <OBJECT type="BOOK-LIT-FORMAT">
                <ID type="ISBN">8374-39384-38472</ID>
                <NAME>A book of James</NAME>
            </OBJECT>
            <OWNER>
                <OBJECT type="Person">
                    <ID type="US-SSN">103-74-8843</ID>
                    <NAME>Mike the man</NAME>
                    <ADDRESS type="email">mike@man.com</ADDRESS>
                </OBJECT>
            </OWNER>
            <PARTS>
                <WORK>
                    <OBJECT type="Chapter">
                        <ID type="relative">0</ID>
                        <NAME>Chapter 1</NAME>
                    </OBJECT>
                </WORK>
            </PARTS>
            <RIGHTSGROUP name="Main Rights">
                <DESCRIPTION>Rights granted to John Doe</DESCRIPTION>
                <BUNDLE>
                    <TIME>
                        <FROM>2000-01-27T15:30</FROM>
                        <UNTIL>2000-01-27T15:30</UNTIL>
                    </TIME>
                    <ACCESS>
                        <PRINCIPAL>
                            <OBJECT type="Principal-Certificate">
                                <ID type="MS-GUID">7BD394EA … </ID>
                                <NAME>John Doe</NAME>
                            </OBJECT>
                            <ENABLINGBITS type="sealed-des-key">
                                <VALUE size="512">lnHtn … </VALUE>
                            </ENABLINGBITS>
                        </PRINCIPAL>
                    </ACCESS>
                </BUNDLE>
                <RIGHTSLIST>
                    <VIEW>
                        <ACCESS>
                            <PRINCIPAL>
                                <OBJECT type="MS Ebook Device">
                                    <ID type="INTEL SN"> Intel 280…</ID>
                                    <NAME>Johns Computer</NAME>
                                </OBJECT>
                            </PRINCIPAL>
                        </ACCESS>
                    </VIEW>
                </RIGHTSLIST>
            </RIGHTSGROUP>
        </WORK>
        </BODY>
</XrML>
```

Figure 12. Sample listing in XrML. [193]

ODRL - The Open Digital Rights Language is said to provide the semantics for a digital rights management expression language and data dictionary pertaining to all forms of digital content. It was originally developed by IPR Systems from Australia and aimed to become a widely accepted standard. The ODRL is a vocabulary for the expression of terms and conditions over digital content including permissions, constraints, obligations, conditions, and agreements with rights holders.

Like XrML, the ODRL is also positioned to be extended by different industry sectors (e-books, music, audio, mobile, software, and so on) and to be a core interoperability language. It has well structured and detailed high-level documentation. Unlike XrML, ODRL is developed in the spirit of open source software and without intellectual property claims. It does not have any license requirements, but XrML patents may cover ODRL also. Compared to XrML, ODRL is a newer challenger. Version 1.0 was released in late fall 2001. Since then, however, ODRL has matured and version 2.0 is expected to be released soon. Open Mobile Alliance, an organization of more than 300 mobile operators, device and network suppliers, information technology companies, and content providers, has chosen ODRL as the rights expression language of OMA DRM standard.

```
<rights>
   <context> <uid> ... </uid> </context>
   <offer>
      <asset> ... </asset>
      <permission>
         <permission-type>
            <requirement>...</requirement><constraint>...</constraint>
         </permission-type>
         <condition> ... </condition>
      </permission>
      <party>
         <context> ... </context>
         <rightsholder> ... </rightsholder>
      </party>
   </offer>
   <agreement>
      <context> ... </context>
      <party> ... </party>
      <permission> ... </permission>
      <asset> ... </asset>
   </agreement>
</rights>
```

Figure 13. ODRL Foundation Model in XML according to ODRL specification [90]
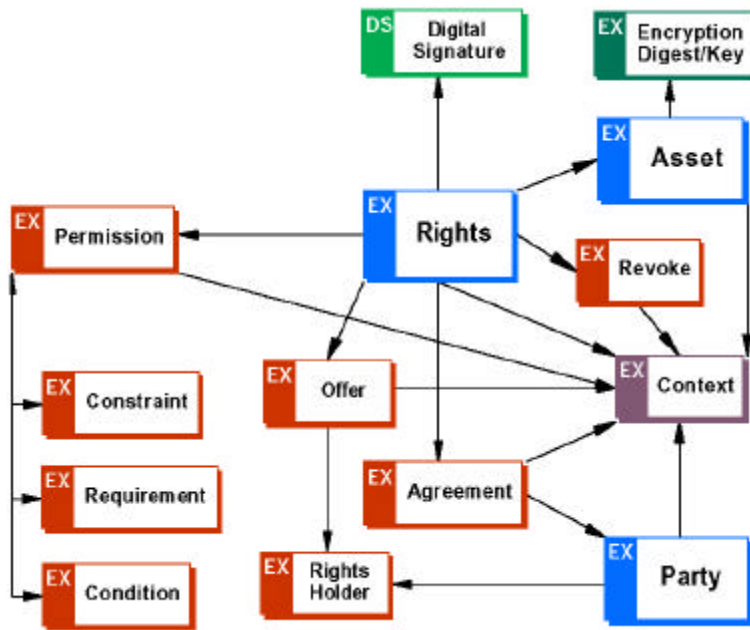
Figure 14. ODRL Foundation Model according to ODRL specification [90]

A couple of important problems related to rights description languages still need to be discussed. First, it is possible to describe very complex sets of rules using those powerful and expressive languages. A rights description resembles a computer program – and why not – it is meant to be understood by computers. For a human being, it can be difficult to understand what those complex sentences mean. However, when somebody buys an information product, it is essential what rights are licensed or assigned. Even if the customer gets the right data, but does not get the rights needed, the customer does not get what was expected. Especially in those countries that have strong consumer protection laws, it is important to inform a consumer in advance what is to be sold. But even if the buyer is not a consumer – but e.g. a company – the transaction must often be cancelled if the buyer does not get what it was anticipating.

Therefore, it would be important to be able to let the buyer understand what is described in the rights description language, but in general it is difficult. It is not enough that if a DRM tool finds out that a certain operation is not allowed, it only

gives user an error message telling something like "Operation not allowed" or "Error in certificate line 798." User should be told why the operation was prohibited: a message like "You are not allowed to copy the document because you have already made all the three backup copies that the license grants" would be much more informative. However, a general automatic translator that would produce a clear description of rights in a human language is probably impossible unless the rules are considerably restricted.

The second untouched problem is the lack of general *ontology.* Each legal system as well as – for instance – all those rights expression languages form a conceptual system of their own. For example, concepts like 'author' or 'use' have somewhat different meanings in different legal systems and some of them, like 'fair use,' may be non-existent in one system while most important in another. To be able to use a DRM system in a number of legal systems, it would be fundamental to share the same concepts.

It is not possible to change all the legal systems to use the same concepts. It is hardly possible to build even a general, universal ontology that would define all the important concepts in all the jurisdictions. That ontology could be used to translate terms between systems, rights description languages and so on. Also, many jurisprudence scholars have published comparative studies that analyze differences between legal systems but they are not general enough and not meant for this purpose.

Actually, it is not possible to define precisely all the legal concepts even within one single jurisdiction. Therefore it is impossible to create a general universal legal ontology. The only reasonable way to achieve common understanding is to accept that there are many coexisting ontologies and try to find some correspondences between them. This could enable the creation of a DRM system applicable in several jurisdictions – in a limited way, of course.

In addition to a rights expression language, entities need a common understanding how to transfer data from one entity to another. One of the most important requirements on the DRM technical tools is that they are interoperable

enough in a network environment. Therefore at least a defined set of communication protocols is required.

Technical protection systems are mostly in product level and meant to assist on product level rights management. They include software tools for authentication, access control, integrity, watermarking, and so on. In most cases, encryption is an essential part of these tools. Many technical protection systems need hardware support. For instance, it is not possible to make a perfect copy protection system without hardware support – not to say that it is possible even *with* hardware support. The most effective solution, a globally tamperproof hardware, is not easy to develop and standardize. Therefore it remains questionable whether reasonable technical protection systems are possible to implement. There are also other serious concerns related to technical protection including for example usability issues: technical protection systems tend to make products less usable and thus less attractive to customers.

Oftentimes, it is not necessary to prevent unauthorized copying. In many cases, authors would like to see their works spreading everywhere. Instead of restricting copying they can be concerned about their moral rights, for example, that they are mentioned and given credit where it is due. In these cases, technical tools do not need to prevent copying, but they should take care of the moral rights of the authors.

Technical tools to protect certain information products gain special legal protection based on Articles 11 and 12 of the WIPO Copyright Treaty. According to those articles many countries have provided legal protection against the circumvention of technological measures that are used to protect copyright as well as against those who remove or alter rights management information without authority. Yet, there are unsolved questions concerning the legal status of technical protection systems [111]. Those statutes do not require that the technical tools are of high quality. In fact, almost any kind of technical protection system is protected. InfoSoc Directive in EU requires that technological measures need to be "effective" to gain legal protection. Directive defines "effective" as "achieving the protection objective." However, a technical measure does not need to be capable of always achieving the

protection objective – otherwise it would not need legal protection. Actually, it seems that in general a technical measure does not need to be too effective to be protected. For example, in Finland, the first Government bill attempting to implement the directive into national Copyright Act (HE 177/2002, later annulled) explained that it is not usually possible to circumvent an effective technical measure by mistake. To me, a technical measure is not very effective, if it is sometimes possible to circumvent it by mistake. Isn't it poor engineering to develop a content protection system that is possibly circumvented by mistake? This raises interesting questions about the role of legal system: does it really make sense to patch up poor engineering with laws? [145]

Rights management systems on an organization level are used to support activities within the organization. A trivial example would be an information management system to manage information on acquired rights and license agreements. Another example would be a verification server that distributes certificates for the end-users to use products that have bought or otherwise got a right to access the information. [107]
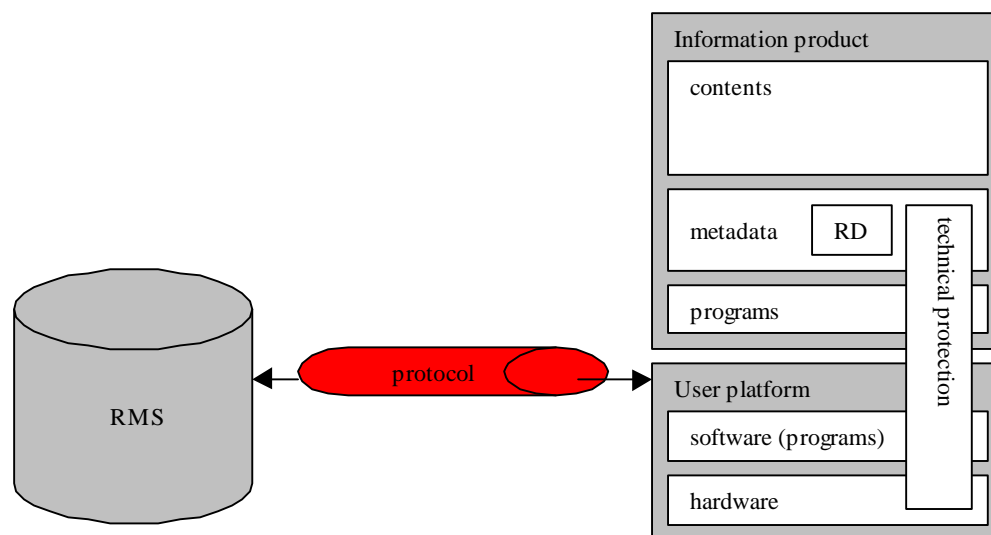
Figure 15. Technical tools in digital rights management.

In Figure 15, an information product consists of contents, metadata and possibly computer programs. An entity accesses the information product using a user platform, which includes hardware and software (i.e. computer programs and data). The technical tools include e.g. the rights description part (RD) of metadata; technical protection tools consisting of metadata, software, and hardware; and the rights management systems (RMS) of intermediaries and originators. The technical tools communicate with each other using a communication protocol.

OTHER FUTURE TECHNOLOGY ATTRIBUTES

Many other interesting and important fields of technology are also developing rapidly. A number of them are still hidden in the laboratories of universities and R&D departments of companies. Yet, some of the major trends are already visible.

They include, for example, the technologies that make use of location information. When either user-devices or a network service can find out where the user is physically located, it is possible to provide services that take advantage of location. While computer networks in general have significantly released people from the boundaries of the physical world, mobile information products and services can in turn make use of physical locations.

Another trend is the progress of technologies to support information adaptation. It will be necessary to manipulate content information based on several reasons. They will include for instance, device features, user profiles, context information, and content's own characteristics as well as service properties.

Also, the technologies that enable ubiquitous computing are becoming important. They extend the reach of computation and information beyond the traditional framework of a computer application running on a fixed set of machines. The extension may be physical, breaking the ties of the desktop, wired computer. Alternatively, the extension may be in scope, providing information services to the public in a form that does not require technical expertise. [181]

SCENARIOS

INTRODUCTION

Scenarios are useful tools for researching future phenomena. They are descriptions of which – in the author's view – are possible futures. It must be emphasized that they are not predictions. Instead they are depictions that are useful to clarify our thinking on the future. [74, 178]

Numerous scenarios are created for various purposes. Depending on the presumptions and purposes, the scenarios may give very different portrays of the future. Therefore, it is important to notice what the scenarios are made for, what presumptions they include, and what are their limitations before using them.

Scenarios are different. Some of them are very small. They simply describe an episode, an event, or a use-case concentrating for example on a person, a business, a product, or a service. They more or less ignore the society at large. They answer questions like, what a future person might do at home or what features a future product will have. I call them *micro scenarios*.

On the other hand, large scenarios, those that I call *macro scenarios*, present conceptions of the world – or at least of a society. They combine a number of attributes and form a large picture on what will happen if these values of the attributes co-exist in the given time. For a company, they illustrate the future operational environment. They give answers to questions like, what the environmental, political, economical, or health-care status will be in 2050, how the

unemployment will develop in the next two decades, or what kind of European Union there will be in 2100 and will the USA still exist.

MOBILEIPR MICRO SCENARIOS

In this chapter, I am presenting a selection of scenarios that we have created in MobileIPR project using the process described earlier. I have slightly modified them to fit better into the scope of this thesis.[1] I analyze them to show what kind of legal challenges will arise in the context of this thesis.

Table 1. The attribute-coverage of the scenarios.

| Scenarios | Factors and Attributes | | | | | | | | | | | | | | |
| | Technology | | | | Economy | | | | | | Society and individuals | | | | |
	Moving user	Context-awareness	Content adaptation	Ubiquitous computing	Dynamic capabilities	Intangible resources	Flat hierarchies	Network economics	Lock-in	Branding	Globalization	Market culture	Political systems	Mind and behavior	Changing work
Weather service	X	X	X			X			X						
Shared pictures				X	X	X	X	X		X	X	X	X		X
Health monitor	X	X		X		X			X		X	X		X	X

I try to cover all the important attributes in scenarios. In MobileIPR project, we created a number of scenarios, but it is unnecessary to describe them all in this thesis. I have chosen three scenarios that best illustrate the factors and attributes discussed above. Table 1 above illustrates how the scenarios cover the attributes. An X means that the corresponding scenario exemplifies the attribute.

SCENARIO 1: WEATHER SERVICE

Description

In this scenario, a user has a service agreement with a Mobile Internet Service Provider (MISP). The MISP's portal includes a weather service that is actually provided by a Weather Service Provider (acting as Mobile Application Service Provider, MASP). The data for the weather service come from Weather Data Providers and are aggregated and refined by the MASP. The user moves beyond the geographical area covered by the MISP and connects to a local Access Operator. The service should adapt to the local context and give information about local weather.

Where does the adaptation take place? It might make most sense to adapt the weather service as near the user as possible, i.e. by the Access Operator. In addition to the users themselves, only the Access Operators know for sure their location. However, the Access Operator does not necessarily know enough about the service to make the adaptation. Therefore it may be necessary to move the adaptation of the service up to the Weather Service Provider, which on the other hand probably does not have information about the user's location.

---

[1] The original versions of MobileIPR scenarios can be found in the project's final report [122].
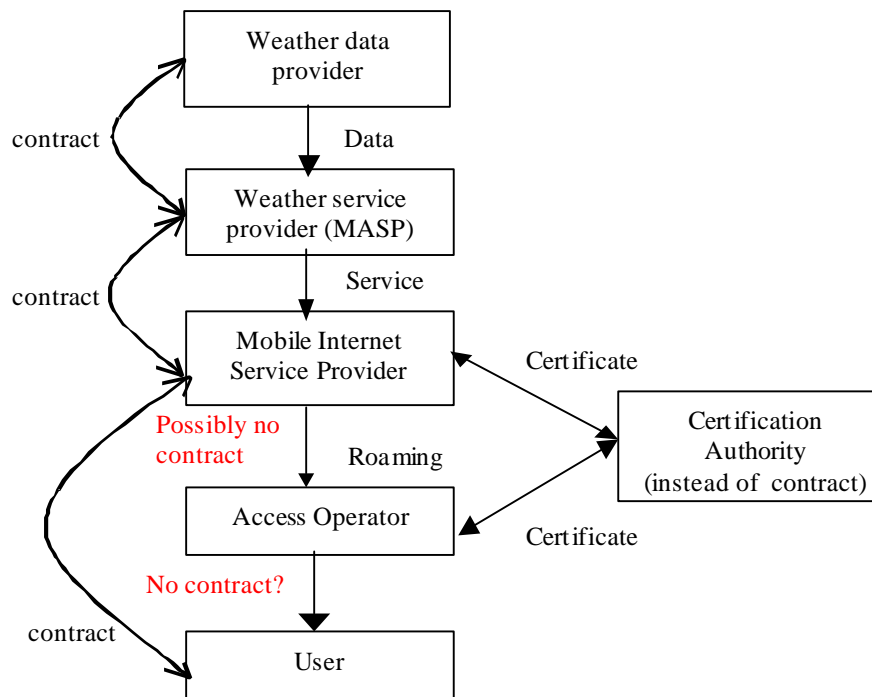
Figure 16. Weather Service

Legal Analysis

Contracts. Who is authorized to adapt the content? It is possible that the Access Operator does not have an agreement with the user nor with the MISP or MASP. It is also possible that the context information is transferred from the Access Operator to either the MISP or the Weather Service Provider and they adapt the content.

If the Access Operator does not have an agreement with the user, it is questionable whether it is allowed to disclose the end-user's location and other information. Technically, it might not be the optimal solution to adapt content far away from the user. If the end-user's mobile device has information about its location, it is possible to make the end-user disclose position info directly to the MISP or the MASP. In that case, user's privacy is smaller an issue. However, technically it is still not optimal to adapt content that far.

Technically the problem could be at least partially solved using metadata. For example, the Weather Service Provider could first send to Access Operator only metadata on what kind of information is available. Based on the metadata, the Access Operator requests information that is appropriate for the context. With that information, the Weather Service Provider sends also metadata describing how the information can be adapted. Legally however, it still remains questionable how the parties make sure that all the rights are respected and how the terms and conditions are obeyed if there do not exist appropriate contracts.

In general, on the Mobile Internet it is not quite deterministic in what way information flows from a sender to a recipient. It is not possible to precisely predict which parties will take part in the chain and therefore making agreements in advance can be difficult. Also, it can be difficult to define what the subject of a contract is. For instance, if contracting parties want to make an agreement about intellectual property rights, but they cannot be sure if any right covers certain subject matter, the contract is not on a solid legal base.

Intellectual Property Rights. What is the legal status of the information? There may be different kinds of Intellectual Property Rights involved in weather information. Though the basic weather data is hardly subject to copyright it might be covered by database protection in the countries that have such a law. Database protection does not cover individual data items but the database as a whole. Certain edited parts of information can be copyrighted. The more original information is included in the service, the better legal protection is achieved.

For example, a third party could establish a competing weather service, make unauthorized copies of valuable information, and further distribute them, but adapting, copying or distributing copyrighted parts requires often the consent of the copyright holder. The service can also be trademarked so that adaptation is not allowed with a claim it came from the original source. Some parts of the service could be patentable as well. If adaptation or copying touches patented parts, it is not possible without permission.

International private law. It is difficult to predict which jurisdictions are involved in a transaction on the Mobile Internet. The applicable law, the competent court, as well as the competent enforcement authority should be decided. As the laws are quite different, the legal interpretation of a transaction depends on the jurisdictions involved.

SCENARIO 2: SHARED PICTURES

Description

This scenario is about sharing pictures between users. Imagine digital cameras with wireless Internet connection or indirect connection via e.g. Bluetooth technology. [171] A user can allow others to access pictures inside his camera. This is done without any other services but the file sharing software in the camera and the basic network infrastructure.

Think about the following scenario. Jaakko takes a trip to Mexico; he can immediately publish in his camera some of the pictures he is taking. His friend Gina can access those pictures instantly. Jaakko is also interested in birds. His pictures on rare birds quickly spread on the Internet.
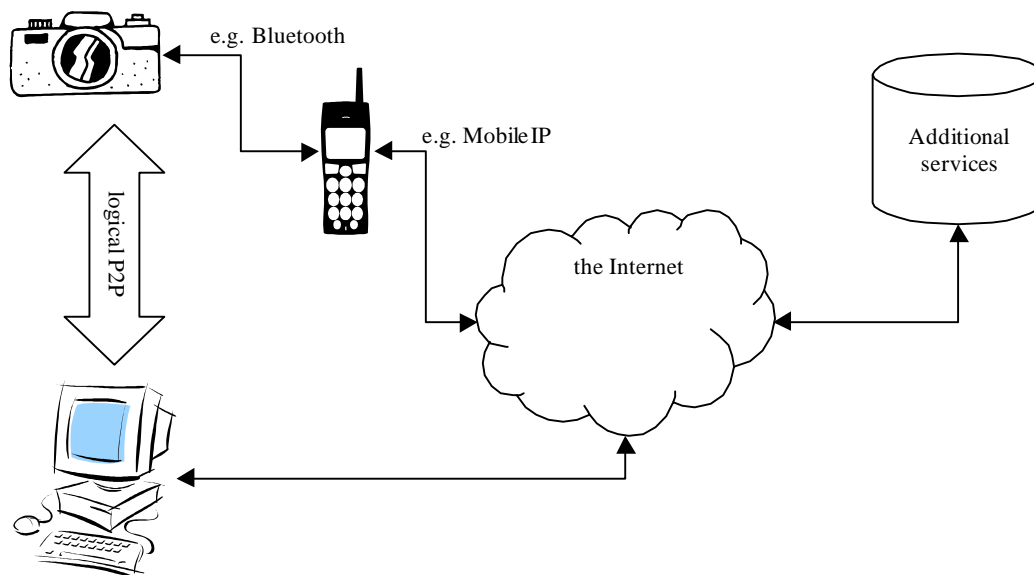
Figure 17. Digital camera and shared pictures.

This is a typical example of a peer-to-peer (P2P) distribution model. However, it is possible to include value-adding third party Internet services. For example, there could be a printing service: a user could order high-quality paper copies of selected pictures by sending them to the printing service on the Internet. Or there could be an editing service: cameras include only limited picture editing capabilities because editing requires powerful computers and sophisticated applications. Those could be accessed through the Internet using the camera as a user-interface. Business opportunities seem endless. It seems natural that this kind of mixed P2P and B2C (business-to-consumer) model will be quite common. Users will interact and share information with other users without commercial services other than the infrastructure, but they will also buy additional services when needed. Commercial providers, on the other hand may utilize the same technologies and sell their information products, pictures in this case, through the P2P network.

Some professional photographers and other content producers may find P2P models changing their ways to work. Imagine José is a professional photographer. He started his job as a hobby, but soon he realized that people are willing to pay for his

pictures. So he started to commodify the pictures he is taking and now makes his living by traveling after crises around the world to take demanded news-pictures in distant locations. Occasionally he is also taking pictures on events or famous people. The Mobile Internet will change his work in many ways. First of all, he will not need a large organization or a back-office. He will be able to sell his pictures directly from his camera to the public. He may join other photographers and form a loose group to coordinate their work and especially to build a brand for marketing purposes. The group could harmonize their infrastructure and offer the customers access to a larger number of photos using the same systems.

Are there limits to the effects of this development? If José is not only a good photographer but also an idealist, he might shake the political systems. His pictures on injustices and unfairness could make people to realize how they are treated poorly. The borderless Mobile Internet will be a difficult challenge for autocratic governments willing to censor the information.

Legal Analysis

First, depending on the content of the pictures there can be identified several kinds of legal challenges.

Fine art. A picture as such can be valuable. It may be creative and original, or it may include important information in itself. If it is original it can be copyrighted. Some jurisdictions also provide specific rights to photographers (e.g. Finnish Copyright Act 49 a §). The photographer may decide who can copy and distribute the pictures and on what conditions. Yet, sharing pictures in a peer-to-peer fashion on the Internet makes it difficult to enforce these rights.

Pornography. A special case is extremely demanded pictures such as pornographic and erotic images. Their economic value means commercial publishers have interest to manage rights in them. In the scenario described above however, the photographers are not likely to sell porno pictures. Instead they might sometimes take pictures in private occasions that other people would

consider erotic or pornographic. The legal challenge is to make sure that these pictures are not distributed against the will of the people they show.

Event. It is common to restrict photographing and televising in some events, like concerts or sports competitions. That is because organizers want to get revenues by selling rights to photograph and televise to media companies. Interestingly those rights are based on contracts, not intellectual property law. To claim that somebody has infringed contractual rights the plaintiff needs to show that there is a binding agreement. If an ordinary consumer goes to an event and takes pictures, it may be difficult for organizers to show that there is a binding contract that forbids photographing. On the other hand, if a person is able to share the pictures on the Mobile Internet directly in the event, it can be troublesome to even find out, who the photographer is, and it does not necessarily help much to later learn who took them, because the economic effects have already occurred. A possibility to get damages from a random private person is not relevant. The legal challenge is to manage photographing and televising rights also in the new situation. Otherwise the organizers have to develop new business models to get revenues some other way.

Paparazzi. People are willing to pay for candid photographs on celebrities. Therefore it can be worth to aggressively pursue famous people to get outspoken pictures on them without consent. This will become easier, faster and thus more profitable using the Mobile Internet. Legal challenges in this area are not different from those with current paparazzi, but they will become more serious. They include issues related to right of privacy and right of publicity that in turn can be quite different in different jurisdictions.

Birds. A number of pictures are documentary and related to hobbies in a way that they do not represent a great monetary value. Instead they can be important in a certain social context. For example, a picture on a rare bird can prove to ornithology community that the photographer actually saw the bird. The legal challenge is related to moral rights: the photographer should have a right to be recognized as the one who took the picture.

Family pictures. Again, some pictures like those on relatives and personal occasions have hardly any value to outsiders, but they can be important to photographers and their family members. The legal challenge is again related to moral rights, but this time the emphasis is on how pictures are used. Pictures can also include private information, for example, on places where somebody has been or on someone's habits. The legal challenge is to make sure that no-one's moral rights and privacy are infringed. It should be noted that data protection law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. Also, the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression is only partially governed by the data protection law. Therefore, many pictures in this scenario are to a degree out of the scope of data protection law. However, if other than journalistic or artistic pictures are published in a computerized mean so that anybody can access them, it is considered to be the processing of personal data under the data protection law. Consequently, the applicability of the data protection law depends in this scenario often on whether anybody is able to access the pictures or whether the access is restricted to friends and family members, i.e. to purely personal or household activities. Also, as discussed above, privacy is protected by a number of laws other than data protection law. It may violate law to process pictures on private people even if data protection law is not applicable, but the picture, e.g., invade against personal reputation. [140, 152, 166]

Pictures on other works. A picture can also be a copy of another copyrighted work. Digital cameras make it easy to copy and distribute any works of visual arts or literary works.

Next, legal challenges in this scenario can be grouped according to legal areas. In each area I further analyze the challenges from the viewpoint of different actors. The legal interpretation changes if the photographer is an amateur or a professional. Also, device manufacturers as well as operators, other intermediaries, and service providers have different perspectives on legal challenges.

Copyright issues at large are important especially to those who want to get profit from information. In this scenario, the professional photographer is the most interested in copyright. It includes particularly photographers' exclusive right to make copies of pictures and the right to distribute them. Also, moral rights can be important in particular for an art photographer. Moral rights, where enforceable, include for example the right to claim authorship of the picture and to object to any distortion, mutilation or other modification of the picture, which would be prejudicial to photographer's honor or reputation. Intermediaries are careful not to be liable for copyright infringements. Other actors, like device manufacturers and service providers, can find business opportunities by enabling copyright protection.

Other intellectual property rights may be significant. Especially database protection can be important in respect to the scenario because pictures in a camera may form a database. Trademark is essential if photographers wish to build a brand as described in the scenario.

Privacy is very important for private persons. In this scenario, it concerns mostly amateur photographers. The other actors should make sure that they do not infringe people's privacy and that their systems enable appropriate privacy protection.

Labor law, in this scenario, affects professional photographers and their employers. In many countries, labor laws are badly outdated in respect to this kind of scenario. They are hard to apply in situations where working hours, company or group formation and other conditions are extremely flexible. Also, international issues will be significant. If a professional photographer travels rapidly around the world, it is not clear which country has jurisdiction over his employment.

Tax laws face similar challenges to labor law. Traditional tax laws are hard to apply in new kind of transactions on mobile networks. Especially consumption taxes (value-added tax, VAT in Europe, sales taxes in the USA) pose significant difficulties in international e-commerce as there are major tax-

related differences between countries. It is also unclear which tax collection authority or *fisc* (a country, a state, a congregation, a community, or another entity that has a right to receive taxes) has jurisdiction to tax certain transaction. [35]

Contracts affect everybody in this scenario. Laws become easily outdated and they cannot be revised quickly enough to follow the rapid development of technologies. Thus some of the legal problems must be solved in contracts. However, all actors do not know each other on the Mobile Internet. It can be even impossible to predict who will be the other parties in a certain transaction, because they can be moving and the connections are changing. To agree on rules within the community by using contracts requires easily an exponential number of agreements. This in turn, increases transaction costs rapidly. In many cases, it would be tempting to use a legal entity (a cooperative, a corporation, an association, or so on), which the members of community could join and which has clear decision-making processes and bylaws that replace the contracts.

Criminal law is the ultimate legal protection system. Typically photographers do not face criminal law in their everyday life, but it remains the eventual legal solution.

SCENARIO 3: HOME-CARE AND HEALTH MONITORING SERVICE

Description

In this scenario, a health care organization (HO) – like a public health care system, a hospital, or a health maintenance organization (HMO) – is responsible for the health care of a group of individuals. The demand for such services is increasing because of the aging population. The responsibility can be based on an obligation under public law or under a contract. Mostly to reduce costs, HO makes a subcontract with a Home-Care Service (HCS) so that the HCS provides some of the individuals with home-care that HO is responsible for. HCS can, for instance, take

care of a senior citizen that does not need to be hospitalized but needs daily visits by medical personnel. The responsible physicians are still within HO, but nurses and support personnel that provide daily care are employed by HCS. The scenario covers both B2B relationships (HO—HCS) and B2C relationships (HO—patient and HCS—patient). [94, 96]

As parts of health and home care services, a number of information products and services are provided. In many cases, actual service provisioning takes the form of information exchange: for example, information on a patient is sent to the service provider, and advises and instructions are returned to the patient.
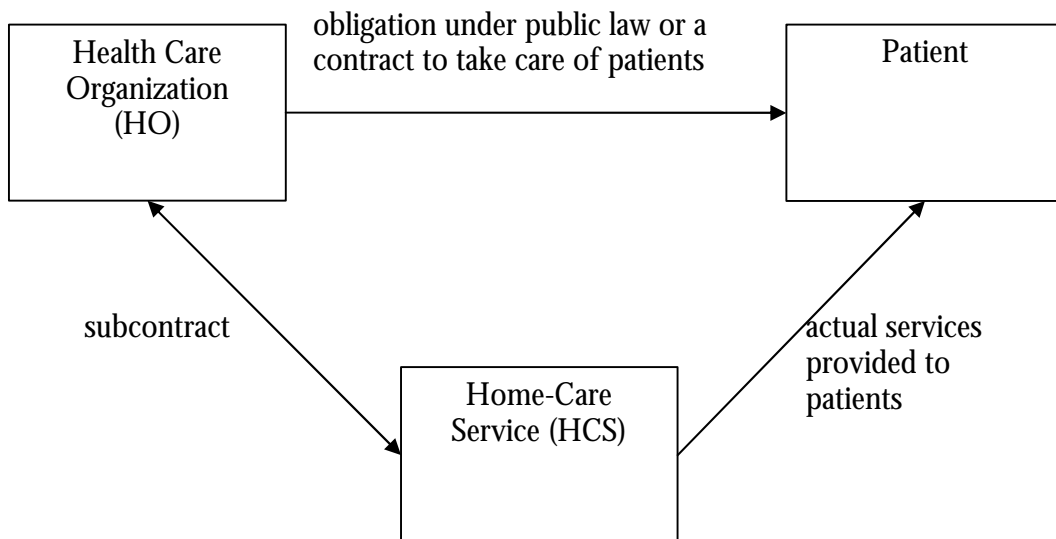
Figure 18. Relationships between the parties in the home-care service example

A home-care service by its nature is mobile. The personnel are constantly moving between, for example, homes and the office. Often their schedule has to be changed during a day due to the unexpected needs of the patients. However, conventional technologies and operational models do not especially support that kind of dynamic and mobile work. The usage of personnel is inefficient, response times are long, and changes are hard to make. It is often difficult to get the right information when needed. The knowledge base is huge and it is impossible to keep

all the important information within reach when home-care personnel are visiting patients. Instead, they often have to go back to the office to get more information. Same applies to authorization issues: in health-related services, it is crucial that a person is authorized to accomplish a certain action. In changing situations, it is often necessary to go back and ask for permission to complete some measures. That is inconvenient at least.

Wireless technologies can improve the service remarkably. The personnel are always connected with the office and they can instantly get new directions and information as the tasks change. They can immediately contact physicians at HO whenever a patient needs doctor's help or additional authorization is required. [27]

In a more advanced system, patients can also be equipped with wireless devices that help them to communicate with HCS personnel or even automatically call help. That might include a set of wearable sensors that send information about person's vital functions to a control center. Optionally some of the sensors can be installed inside customer's body. The service sends reports and instructions how to improve their health. In the case of emergency, the service can call an ambulance, a doctor, or other help provided it gets patient's location information. The customer could even be equipped with a dosage device so that with the permission of HO's physician HCS control center can remotely give for example insulin, vitamins and micronutrients or heart medicine when needed. [27, 96]

The capabilities of the service are heavily based on information. First, a lot of information is extracted from the users and stored in the service. Second, a large computerized knowledgebase is used to help the doctors to make decisions and even to automate some choices. Third, the doctors and other professionals within the service obviously use their own knowledge to help the customers. All this information can be valuable and therefore the service operator can be interested to sell it further. Perhaps it is possible to fund the service by selling such information to other entities. Also, this kind of sensitive personal information can be attractive for malice usage. So, it is an essential question, which one should be able to control this valuable information: patient, HCS, HO, or someone else. [27, 96]

Health services have traditionally been very local. A doctor cannot serve people in a very large area. However, the service described in this scenario is not geographically limited. It could be offered to the customers around the globe.

This scenario represents a sample application of ubiquitous computing. New business models are also involved. Some important mental aspects should be considered, like how the users feel if some unknown people in a control center, "a big brother", even with their permission, is always monitoring them and knowing better than themselves how they are doing. This might be also an example of changing work. A doctor can be sunbathing on a beach while on duty. In an emergency, the doctor gets all the information on the patient, including the medical history and the current condition, and is able to interview the patient using a mobile terminal still lying by the sea. [e.g. 27]

Legal Analysis

Contracts. In this scenario, just like in the previous two, contractual issues may become central. HO and HCS probably have a contract that specifies the processes they use. For instance, the contract may state the procedures that HCS must follow when new instructions are needed. HO is liable and therefore it has to make sure that HCS adequately acquires the instructions and follows the rules. The contract cannot give too many liberties to complete the tasks. Therefore it easily solidifies the processes and makes them hard to change.

International private law. If the service is provided globally or if a customer travels abroad while using the service, international aspects become vital. Laws concerning health services are quite different around the world so it may have a vast impact on the service under whose jurisdiction it is.

Intellectual Property Rights. In this scenario, intellectual property rights do not protect remarkable portion of information. Information on a customer, a single advise from a physician, a control message from the control center are important, but hardly protected by copyright or other intellectual property rights. The more

information is collected into a database the more likely the whole base is covered by database protection. Refined advises, edited messages, and sophisticated automation programs are also more likely to be copyrighted. Therefore intellectual property rights will be more important in this scenario if the service is further developed towards a more mature system that not only transfers data, but stores and distributes refined information in a stylish way.

Privacy. Large part of the information managed in this scenario is private by its nature. People do not want to see information on their health spreading around. Therefore the system must support privacy and confidentiality extremely well. On the other hand, many companies and public agencies would be interested in accessing those data. For example, a commercial company would be able to direct marketing quite accurately to right individuals if it knew that much about their habits and health as this system knows. Some customers might be willing to benefit from the situation while others are so concerned about their privacy that they would not dream of letting this service to sell the information. In European Union, the data protection directives [140, 146] have set quite strict rules, but in the USA, for example, the discussion about privacy protection has not led to comparable statutes so far.

Professional Negligence and Torts. The scenario presents a situation where physicians and other experts have a remarkable liability on people's health and life. It is extremely difficult to make this kind of a system completely reliable. In some countries, the potential damages based on medical malpractice or products liability could be enormous. In general, entities that offer expert services through the Internet may be accused of professional negligence. It is possible that the legal risks prevent this kind of services even if both the customers and potential service providers want them. In addition, many countries have strictly limited who is allowed to give medical services in their jurisdictions. A service like the one described here would possibly conflict with these rules.

MC2 SCENARIOS

HIIT's Mobile Content Communities (MC2) project has created a set of scenarios to study future gaming communities. I have not participated in the creation process. Instead, I have analyzed the scenarios from the legal point of view and given comments to the MC2 project team. MC2 project is managed by Dr. Marko Turpeinen, and the researchers who have mostly contributed to the scenarios are Risto Sarvas, Tero Laukkanen, Antti Salovaara, Fernando Herrera, Kai Kuikkaniemi, Kalle Toiskallio, and Mikael Johnson. The complete scenarios are in Appendix 1, but short synopses are also included below in front of each legal analysis.

SCENARIO 1: CREATING A STORY FROM MIXED-REALITY GAME SESSION

Synopsis

Two players, Jake and Samuel, spend their evening in a hockey game they have placed bets for in a company facilitated betting community website. During the game they buy a new bet and combine it to their old ones. After the game they re-experience the winning goal from video, and in the end create a memorabilia artifact, i.e. a video, and share it with other people.

Legal Analysis

Betting

Betting is a highly regulated field. Most countries seem to have laws that regulate betting. In Finland, the Lottery Act applies to betting. Betting is typically subject to license, often monopolized by law, and in many jurisdictions even totally prohibited. In Finland, in accordance with the Lottery Act 6 § and 11 §, betting is the monopoly of Oy Veikkaus Ab, the government-owned pools company. [43]

In addition, marketing laws often include rules that limit the use of lotteries. Roughly speaking, the marketing rules governing lotteries and competitions on computer networks can be classified as the following table shows.

Table 2. Marketing rules on lotteries and competitions.

Participation Prices	Free of charge	Chargeable
Nonrandom	Consumer protection laws may limit	Mostly ok
Random	Consumer protection laws may limit	*Highly regulated, often prohibited!*
No price	Mostly ok	Mostly ok

Liability for incorrect information

"Hot tips", if they are incorrect, may cause liability. However, that is unlikely, if their authoritativeness is not emphasized and the user is able to understand their nature from the context – that they are only suggestions and can be incorrect. Obviously, other incorrect information (e.g. a game report claiming that somebody was in a game although he/she actually wasn't) could cause liability for damages, but because there doesn't seem to be any special concerns of that kind in this scenario, it is not necessary to discuss them further here.

Intellectual Property Rights

Creating a multimedia show on a hockey game is legally interesting. From the copyright viewpoint, nobody owns the copyright in a hockey game. How the organizers of games and other events of that kind get the huge televising fees, if they do not actually have any televising rights to sell? Why cannot anybody just walk in a game and televise it?

A sport performance is not a work protected by the copyright law. However, it is a quite established custom to state that the game organizers have an exclusive right to televise the event. Although this viewpoint is hardly supported by the copyright law or any other intellectual property law either,

some indirect support can be found. For example, Directive 97/36/EC acknowledges that there can be exclusive rights in sports events:

> "(18) Whereas it is essential that Member States should be able to take measures to protect the right to information and to ensure wide access by the public to television coverage of national or non-national events of major importance for society, such as the Olympic games, the football World Cup and European football championship; whereas to this end Member States retain the right to take measures compatible with Community law aimed at regulating the exercise by broadcasters under their jurisdiction of exclusive broadcasting rights to such events". [142]

The organizers typically claim that they have an agreement with the audience that forbids unauthorized televising, video recording, photographing, etc. This argument is not always very strong. It may be challenging to show that there exists a binding agreement between the game organizer and each person in the audience. In the USA, for example, there is also a law that prohibits *trespassing*, i.e. unauthorized entry on another's real property. This law allows the game organizer to define the rules to enter the place. The game organizer can prevent a TV company from entering the event. However, it is not self-evident that the game organizer may stop a person from taking pictures or video-recording if he/she has entered the property lawfully. Therefore the legal basis of the right to restrict photographing in an event is not very strong. The televising companies do not usually want to challenge that conception, because they also benefit from the rules that guide the business, although the rules are probably not grounded on law – but merely on *soft law*, i.e. on codes of conduct. Instead, ordinary people, Jake and Samuel, who spend their evening in a hockey game, do not necessarily benefit from the status quo of game organizers and televising companies. They may want to take pictures, create multimedia shows, and publish them. As long as they just take a couple of pictures for their own albums, it does not probably matter the game organizer. However, if they create and publish a multimedia show that competes with the television programs, the game organizer or the broadcasting company is likely to react.

Privacy

The scenario involves some privacy issues. Some of the pictures that Jake and Samuel take of audience can be governed by data protection law. It does not make the pictures illegal, but it may restrict the usage of them.

Right in portraits

In addition to photographer's rights, the one that a picture shows may have rights in the picture. As discussed above, the rule of the thumb is that a picture that presents a person may not be used for commercial purposes (especially in advertisements) without the consent of the person. Instead, the person does not have right to forbid others to use the picture within normal freedom of speech or communication (e.g. news). Yet, the publishing of a picture may never be insulting to the people that the picture presents and the picture must not infringe their privacy. [60]

SCENARIO 2: PLAYER-CREATED MOBILE GAMES

Synopsis

A player wants to make a *mod* (a modification, a change to a published game) but needs help from other players in technical issues.

Legal Analysis

Intellectual Property Rights

A game can be protected by various intellectual property rights. First, the implementation of the game can be *copyrighted*. Thus the copyright-owners have an exclusive right e.g. to prohibit others from "making it available to the public, in either the original or an altered form, in translation or adaptation, in another literary or artistic form or by other technical means". [153] In other words, an adapted game cannot be distributed without the consent of the copyright-owners. If a mod can be

distributed separately independent on the game itself, the distribution of the mod

usually does not infringe the copyright in the game. In some cases, the copyright-owner might argue that the mod's sole purpose is to help players to alter the game illegally. At least in some jurisdictions that could make the mod illegal. Of course, many authors of games and computer programs have accepted also the distribution of an altered game in advance by using specific license terms.

The implementation of the mod, on the other hand, can also be copyrightable. In this scenario, the design of the graphics, photos on the mission locations, and the program code are copyrighted works while the mission structure and tags are probably not. Note that a modified game is a derivative work in which both the original authors and those who have modified it have copyright. That is, the players need a license from both the copyright-owner of the game as well as the mod to be able to play the modified game. The copyright in the mod belongs to the modders jointly. That is, it might be difficult to agree on license terms afterwards, if they have not agreed on them in advance.

Second, in Europe, some games can be partially protected by *database sui generis right*. It provides the maker of a database with the right to prevent extraction and re-utilization of the whole or of a substantial part of the contents of that database. In accordance with the EU Directive on the legal protection of databases, a database is a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. To be protected, there needs to be a substantial investment in either the obtaining, verification or presentation of the contents. In principle, the database of the tags within a game could be protected by database sui generis right if the game developers have invested substantially in it.

Third, a game may include *patentable* inventions. Both the original game and a mod may have them. There are limitations on the patentability of games. Schemes, rules and methods for games as such are not patentable. However, an invention related to an implemented game is hardly a scheme, a rule or a method *as such*. [114, 121]

Therefore a novel invention related to a computer-implemented game, including an inventive step (being non-obvious), and having industrial applicability, could well be patentable. However, the invention is no longer novel, if it has been published. Everything made available to the public in writing, in lectures, by public use or otherwise shall be considered as known and not patentable. When Janet presents her idea to the community, she is likely to lose the patentability of the invention unless the community is very limited and bound by a non-disclosure agreement. On the other hand, patentability also requires that the invention must be technical. As long as Janet's idea is rather abstract and not defined in terms of the technical features of the invention, it is hardly patentable. To patent the invention, Janet should be able to develop the idea and describe it in technical terms with a limited group of people. A game that includes a patented invention cannot be distributed without the consent of patent-owners.

Fourth, a game can be *trademarked*. The names of games are often trademarked. If a trademark protects e.g. the name, then a modified game cannot be distributed using the same name without the consent of the trademark-owner. Note, however, that trademark is related only to business: it is usually not applicable to hobby communities that do not make money.

Labor and Tax Laws

As long as a game is developed in a hobby community and no-one gets paid, the labor and tax laws hardly play any significant role. Compensation even in a form of a "free cell phone" could introduce taxation questions, but would hardly bring up labor issues as far as the payer is not controlling the work. When Janet becomes a part-time employee of the game development company, the labor law is applied. The company may thereon control her work and is also largely liable for it. Also, during the employment, copyright, database sui generis right, and patents are usually transferred automatically to the employer.

SCENARIO 3: A VISIT TO A MOBILE ONLINE ROLEPLAYING GAME

Synopsis

A player has communication problems in mobile game play.

Legal Analysis

Quality of Service

Communication problems may cause damage to users. By default, everybody is liable for his/her own damages. In certain cases, however, a service provider can be liable for the damages.

First, normally there is a contract between the user and the service provider. Liabilities are usually stated and strictly limited in the contract. Although contracts do not limit the liability based on deliberation or gross negligence, typically the liability of the service provider is quite limited.

Second, a special law may govern the situation. For example in Finland, the law stipulates that if a fault prevents the usage of subscription more than 48 hours per month, the operator must reimburse one monthly basic fee. In most cases, this is the total compensation regardless of the actual damages. [157]

Third, tort and liability laws in general may be applicable. Especially, if the one, who has become damaged, is not a customer of the service provider or otherwise in contractual relationship with it, then the damages should be judged in accordance with general tort liability law. Then one should be able

1. to show that the service provider has done something wrong,

2. to show that the wrong is the cause of damages, and

3. to show the amount of actual damages.

These are hard requirements and they can only seldom be fulfilled.

In conclusion, technical communication problems rarely lead to significant damages.

SCENARIO 4: LOCAL SUPER-DISTRIBUTED GAME AND SOCIAL ACCEPTABILITY

Synopsis

There is a wireless local network inside one shopping mall. To tempt new customers to come to shopping mall, the customers can play location-based mobile games with each other using the local network.

Legal Analysis

Intellectual Property Rights

In addition to comments about the previous scenarios, intellectual property rights would likely allow the pricing model described above: a user can first play with a free, crippled version, and then upgrade to a full product. More interesting questions would arise, if someone were able, for example, to crack the game and use the full product without paying anything. Could a user, for instance, win a prize with a cracked game?

Socially unacceptable behavior

Playing a game should not have an effect on person's responsibility to behave correctly. The store personnel have a right to chase away people who trouble others. An exception might be a situation in which the rules of the game that the store has organized or accepted allow or require certain behavior. This is hardly the case in this scenario. On the other hand, the game organizers might be liable for incitement if they intentionally have led users to break the law.

SCENARIO 5: SOCIAL PRESSURE AND CONFLICTING MORAL CODES IN VIRTUAL WORLDS

Synopsis

Also in virtual communities, there may be a role conflict between smaller and larger scale social pressures. 'Traffic' between these two levels might be used for enlightening or even educational purposes. Even if there wouldn't be any explicit moral code not to mention laws in a virtual community, the community itself will draw the borderlines between what is thought to be good and bad.

Legal Analysis

The scenario discusses moral and social rules. It shows the undeniable limitedness of legal rules. The questions arisen in the scenario are hardly solved with legal arguments.

SCENARIO 6: CHALLENGES IN MANAGING PLAYER PRESENCE AND CONTEXT IN A PERSISTENT MIXED-REALITY GAME

Synopsis

Franck has forgotten that he is a member of a conspiracy game. He receives an upsetting call in the middle of the night, and is forced to ponder whether he should quit his participation in the game. The community tries to keep him as a member by showing him simple voting results of his popularity among other members of the community.

Legal Analysis

Privacy

As discussed above, the right to privacy is highly protected in many countries, but the rules are spread out in numerous statutes. In general, private information, such as salary or location, must not be disclosed without the consent of the person. However, some specific statutes may include rules that permit authorities to receive private information. For example, in accordance with Finnish Act on Charges of Social and Health Care Services, the authorities are allowed to get information on the income of kindergarten children's parents from other authorities, banks, insurance companies, employers and so on, but not from e.g. recreational communities. [150]

Privacy is also protected by penal codes. For example, it can be a punishable invasion of domestic premises, if a person unlawfully disturbs the privacy of another by making calls (the Penal Code of Finland, Chapter 24, Section 1). In general, only intentional acts are punishable. Therefore, in this case, if the caller sincerely believes that Franck is willing to participate in the game, it is not an invasion of domestic premises to make the phone call. [152]

Contracts and consumer protection

Consumer protection law permits a consumer to fairly freely terminate the subscription of services she or he might have ordered. The actual rules vary in different jurisdictions.

SCENARIO 7: CONTEXT SENSITIVE ADVERT GAMING

Synopsis

On a visit to a movie theater two girls play a mobile game that has been released as part of a cross-media promotional campaign.

In addition to the above mentioned challenges with marketing rules, consumer protection, and privacy, this scenario does not represent any new legal issues.

SCENARIO 8: COMPANY-COMMUNITY RELATIONS IN CONTROLLING USER-CREATED CONTENT

Synopsis

When an online gaming community matures, there may be a change in power relations between different player groups with different gaming practices, like modding. What's suitable and right for some isn't for others, and one may ask: "whose game is this anyway?" The boundaries between fandom and corporate culture change, and there are increasing difficulties in considering different player groups when developing future versions of the game.

Legal Analysis

The question how intellectual property rights may protect games is already discussed above. In this scenario, IPR and license agreements form a tool to control the community. The "hole" in the license agreement highlights the difficulties in drafting good agreements. It is unattainable to prepare for all the possible situations.

The contractual framework for a gaming community is complex. It is difficult to build binding contractual relationships between all the members of the community. At least, it is laborious, transaction costs increase rapidly, and the management of contracts gets troublesome. In an unpredictable situation, the existing binding contracts hardly enable the community to sentence a rebelling member to sanctions. Therefore it would be better if the community could form a legal entity, such as a corporation, an association, or a cooperative, which has adequate bylaws, reasonably well-defined membership, necessary administration, clear decision-making process,

and an accepted policy to settle disputes among members and between a member and the community.

In the scenario, the community is rapidly spreading all over the world. An internationalizing gaming community or company faces mostly the same legal challenges that any growing company heading towards international markets will meet. For example, differences between marketing, IPR, and competition laws are difficult to handle. Also, problems related to, for instance, international taxation can be severe. Some of these problems arise faster for a company or a community that operates on computer networks than for a traditional company providing material products. However, in addition to the issues already discussed above, the fundamental nature of those challenges hardly depends on information products and is therefore out of the scope of this analysis.

BETWEEN SCENARIOS

In HIIT's Between project the idea of ubiquitous computing or *ubicomp* was investigated from the user's point of view by creating user scenarios and experience prototypes with user-centered product concept design methods. The emphasis was on mobile ubicomp. The project created the total of 48 scenarios. Eight of them were further elaborated, and finally two prototypes were developed based on five of those eight scenarios. [58]

Between scenarios were created by the members of Between project team: Eugene Gryazin, Anu Kankainen, Tomi Kankainen, Antti Kantee, Petteri Kiiskinen, Boris Krassi, Esko Kurvinen, Antti Nurminen, Jyrki Oraskari, Antti Oulasvirta, Matti Rantanen, Michael Samarin, Nikolaj Tatti, and Sauli Tiitta. I have not participated in the creation process of the scenarios, but I have afterwards analyzed them legally. Below, the eight scenarios are described and analyzed more in details, but the remaining forty scenarios are also discussed briefly. [15, 58]

1. *Ubiquitous SIGs* (01-6): Individuals belong to different special interest groups (SIG). SIGs are tagged with location-dependent and -independent services

130

and information. SIGs activate and become visible when members enter a cell. Push-services are listed separately from the activities organized and activated by the members.

2. *Give me a break! Mode-based filtering* (02-1): Context-sensitive push messages are filtered according to modes that are switched on/off either manually or automatically. Others can view the mode you're in. "Meeting is over and Risto heads for lunch. Risto switches to 'Break' mode. Having made his order, Risto sits down. He notes that the restaurant provides jokes for his break. Risto skims through some of the jokes. As Risto returns to the office, the magic thing announces mode switch with barely perceivable haptic stimulus."

3. *Silent push* (02-3): Niina is at Esplanade, she is in a hurry going to her friend in Katajanokka. There is an event with a band and a lot of people, but she does not have time to stop there this time. Her magic thing is in her pocket, silently displaying what is going on in that area. When she moves on further away, this information is automatically erased.

4. *Coffee mug* (04-1): Tero is editing three articles for the next issue of his computer magazine Datalehti. He is in hurry to edit all those articles. He decides to talk with his colleagues who could help him. He stands up from his desk and heads towards the kitchen at the other end of the office. As he takes his coffee mug with him, the coffee mug automatically downloads all the three Word documents currently active or open on Tero's personal computer and beeps three times at a barely audible volume. Tero walks to the kitchen and pours some coffee to his mug. He then walks to Jenni's desk and asks if she could edit the Cruz Broker story.

5. *The Event Tagging Device ("a knot in your finger")* (04-2): Erno and Jussi are having a coffee break at the office. Among other things they are discussing about an article Erno is writing. They agree to meet on Thursday and Jussi promises to forward some related email to him before that. Erno does not have his calendar with him, so he tags the event using his Event Tagging Device. The device is small and it has only one button. The Event Tagging Device records all the

contextual variables it has access to at a time when the button is pressed (e.g. ″Tag 10:30; Location: Coffee Corner; Duration: 17 minutes; Background noise level: low; Present: Jussi, Paula; Devices: JussiPDA, Laserjet 4M″). When returning to his PC, Erno sees list of events he has tagged. Getting a notification from his coffee break with Jussi helps him to remember what he promised to do.

6. *Track Detector* (05-5): Standing outside Stockmann, Pirre gets a notification that that Carl-Johan has just been there. Pirre follows Carl-Johan's trace to railway station and they decide to go to café NetCup.

Figure 19. Between scenario 05-5 [15]

7. *Public votes* (07-2): Public, location-based votes that everyone can create. "Lili walks by the statue called Kolmen sepän patsas, which is under renovation. She notices that there's a voting. 'Should they put shorts on these naked men? By: [Anonymous182] 89 % No – 11 % Yes.' She votes "No", and continues."

Figure 20. Between scenario 07-2 [15]

8.   *Item reminder* (09-1): Liisa is leaving home. She has a Magic Thing with her that knows what items she usually carries with her. The Magic Thing notifies her that she forgot her bus ticket and also the probability of needing a lipstick is 68 %. Liisa takes the bus ticket and the lipstick with her. A Bayes-network has learned what items she usually carries with her when leaving home at a specific time and/or in relation to the forthcoming events she has marked in her diary.

The other forty scenarios present ubicomp applications from restaurant watcher to friendship manager. They are strongly focused on people's everyday situations at home, at work, shopping, and in free time. All the scenarios are very small, like flashes on the future. Each of them focuses strictly on a certain single idea on how the future ubicomp technologies help ordinary people in their everyday life. They do not discuss business models or revenue logics.

LEGAL ANALYSIS

Between scenarios are quite brief. In the legal analysis, I am trying to stay within the wordings of the original scenarios and not to speculate what else could have been described. Therefore also my analysis stays quite concise.

Between scenarios describe very human centric and personal situations. They intend to bring up future product concepts that help people in their every-day situations based on the needs and experiences of individuals. Therefore, from the legal point of view, they highlight privacy and data protection issues. Most of them present situations in which people are sharing their private information, like information on their location, profiles, belongings, or interests, or even 3D models of themselves, with all the other people around. Only a few scenarios explicitly tell that the users are able to district others' access to information (e.g. 01-5: "Sanna and her friends have made their product ID-tags visible to others as part of their public profile.") while most scenarios imply that anybody can access users' private information (e.g. 02-1: "Others can view the mode you're in.") or ignore the issue.

Probably most of the scenarios could be implemented in a way that users' privacy remains protected. That would however make the technology remarkably more complicated. The scenarios clearly show how easy it is to ignore data protection. Many exciting inventions are possible, if private information is available. Yet, those inventions also enable evil usages. If data protection excludes some of the most thrilling possibilities, it also disables severe misuses of private information.

Intellectual property rights are not discussed explicitly in Between scenarios, but some of them lead to think about who is allowed to use valuable information that is produced in relation to scenarios. For example, a personal 3D profile or a collection of them (01-4) might form a protected database. In case the user does not own the rights in the database, but they belong for example to the company that has scanned the body, some of the actions may require permission from the rights holder. Scenario 04-7 *Event tagging photo* implies issues relating intellectual property rights in pictures since the user is willing to pay for a picture.

The scenarios hardly describe any business models or revenue logics. Therefore, contractual, taxation, and many other legal issues remain mostly hidden. The above mentioned *Event tagged photo* scenario (04-7) briefly discusses buying and selling pictures, therefore touching at least on contractual issues. Yet, ubicomp does not introduce any new contractual challenges even in that case.

ISTAG SCENARIOS FOR AMBIENT INTELLIGENCE 2010

The IST Advisory Group (ISTAG) has been trying to get a higher level of focus and a higher pace of development in Europe on Information and Communication Technologies. As a part of this work, ISTAG launched a scenario planning exercise in 2000. The scenarios were developed by the IPTS (part of the European Commission's Joint Research Centre) in collaboration with DG Information Society and with the active involvement of 35 experts from across Europe. The aim was to describe what living with 'Ambient Intelligence' might be like for ordinary people in 2010. [28]
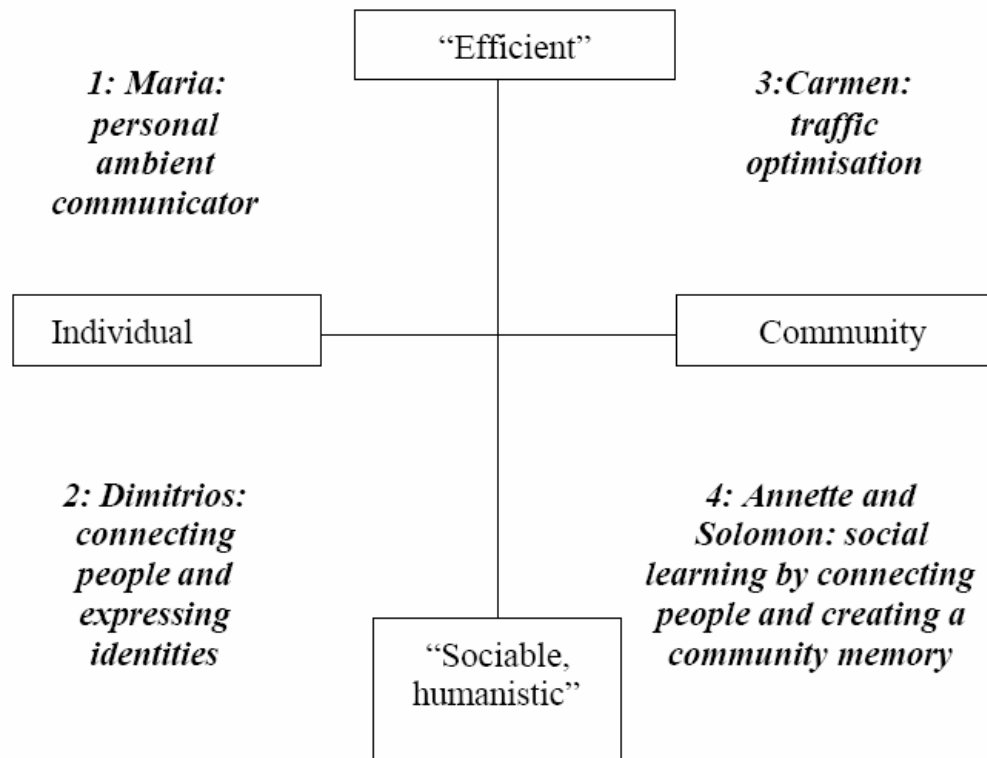
Figure 21. Main structuring differentials between the four ISTAG scenarios.
[28]

The four scenarios that ISTAG created are described in their final report. The descriptions are attached to this thesis in Appendix 2. [28] In brief, they are:

1. *Maria* is a scenario about busy business person traveling abroad and using highly automated communication systems. The lead markets for the technology here are efficiency orientated and less price-sensitive business sector demands. From the legal point of view it is notable that most transactions – both private and public – are automated. Hardly any human interaction is required. Most decisions are made by machines. The context sensitive services utilize a lot of personal information. Especially location information is needed for many services.

2. *Dimitrios* scenario emphasizes playing and social interaction rather than efficiency. Dimitrios has authorized his communication device to filter incoming calls and even to automatically reply to some of them. Other than that most decisions in the scenario are still made by human beings.

3. *Carmen* scenario describes a future world in which vehicles are guided securely on demand basis. It implies major infrastructural developments, like highly developed networks of inter-operating sensor systems and dynamic database management systems. It describes an ambient landscape in which the joint flows of bits and atoms are optimized to create a more sustainable urban system. It also makes significant assumptions about changes in public behavior such as accepting ride shares and traffic management systems. On the other hand, human beings seem to be in control – they make the decisions – and no personal information is necessarily transferred without their consent.

4. *Annette and Solomon* scenario introduces a future studies group set-up. It implies significant technical developments such as high 'emotional bandwidth' for shared presence and visualization technologies, or breakthroughs in computer supported pedagogic techniques. In addition, the scenario presents a social vision of ambient intelligence in the service of fostering community life through shared interests.

LEGAL ANALYSIS

General

The four ISTAG scenarios are quite similar from the legal point of view. They all portray a world in which computing and communication devices are present everywhere and have access to huge amount of personal information. Also, they all describe situations in which machines make decisions on behalf of human beings. In *Maria* scenario, the machines make very significant decisions, like they seem to decide who is allowed to enter a country, and they make binding contracts on behalf of

someone else. In the other scenarios the decisions that machines make are of lesser significance. Because of the legal similarity of the scenarios, they are not analyzed separately, but their analysis is presented below as a whole. As *Maria* scenario seems to be legally the most challenging, I am using it as an example even though the other scenarios fit better to the scope of this thesis. The same observations, however, mostly apply to all ISTAG scenarios.

Privacy

The ambient intelligence technologies described in ISTAG scenarios represent huge challenges to privacy. The interconnected computing devices must have access to a large amount of private information to be able to provide the services. This might poses severe risks to privacy. The scenarios do not refer to any such problems: the system is working perfectly and it honors the users' privacy. Nothing however ensures that. If the system has so much private information about people, it is easy to – intentionally or by mistake – use it wrongfully or distribute it too widely. Actually, often the best solutions from the purely technical point of view are unacceptable from privacy perspective. For example, access control mechanisms that prohibit unauthorized use of information are complex to implement and decrease the overall performance and usability of a system. Therefore it is often tempting to leave such mechanisms away or at least make them as light as possible. Unless a paying customer insists or a law requires, a system provider easily ignores privacy protection.

In the European Union, several directives and other statutes – like for example Directive on privacy and electronic communications (2002/58/EC) – have been issued to protect privacy and personal information. For example, *location data* is essential context information for many ambient intelligence services. The services may adapt to the user's location, and services and information can be made available for the user in the location. However, processing such location information is sensitive and it requires the consent of the user. In an ambient intelligence environment, where a number of services and service providers exist, it is difficult to get the consent from the user to process location data for each service.

For example, article 9 of Directive on privacy and electronic communications: [146]

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

In *Maria* scenario for instance, it seems that most services would benefit from her location data. However, the situation becomes complex if Maria needs to accept separately each service to use the data, and each service must provide her with the continuing "possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each

transmission of a communication". In practice, it would probably be easier for Maria simply not to use the services. Surely, usability studies and automatic mechanisms can make the situation much easier, but ultimately the user must have control and the ability to refuse the processing of location data in order to fulfill the requirements of the directive.

The directives aim at harmonizing legal systems and guarantee certain level of protection within the EU, but obviously they do not apply in countries outside the Union. Therefore, exchanging information within the Union has been tried to make flexible. On the other hand, it is highly restricted to transfer personal data from the member countries to "unsafe" countries outside the Union.

In *Maria* scenario, European citizen is traveling outside Europe. Her personal data mainly originates from the Union but is needed in Asia. Presumably Maria is willing to use those personalized services and therefore accepts the transfer of her personal data between at least her home-country and the Asian country. Yet, in accordance with the directives and European national laws, she has to explicitly accept the transfer of data from Europe to the Asian country. This effectively protects her privacy, but introduces severe challenges to the designers of the services. Also, it decreases the efficiency of the concept that was emphasized by ISTAG. According to ISTAG, "Ambient Intelligence works in a seamless, unobtrusive and often invisible way." The need to get consent from the user makes this goal hard to achieve.

Contractual and administrative law

Maria scenario describes how all the immigration and border control procedures as well as negotiation processes have been automated. In most cases, legal systems assume that human beings make the final decisions: there is a boarder guard to decide who is allowed to enter the country; human representatives of legal entities make agreements on behalf of the organizations, and so on. Those human beings are able to make the decisions even using incomplete information and taking reasonable risks, they are authorized to use due liberation, and eventually they are also

responsible for their decisions. It will take a long time before – if ever – computer systems are able to deliberate complex problems, make answers with incomplete input information, and take intentional risks. There are fundamental difficulties to make a machine liable for its decisions.

When developing scenarios, it is often difficult to estimate how much change can occur in a given time period. As quoted above, according to WIIO's law, people tend to overestimate the near future and to underestimate the far future. [80] In *Maria* scenario, it seems optimistic that the legal systems could change by 2010 that much. Especially with respect to privacy and data protection, the legislation in Europe has gone in a more restrictive direction in the recent years. While protecting most important values it has not made this kind of a scenario easier to achieve. At least, all this will not happen by 2010 as the scenario suggests. Only the easiest, most straightforward cases can be automated. The scenario is legally feasible, if it is presumed that human beings are still making all but trivial decisions.

MACRO SCENARIOS

As I have defined above, macro scenarios are large and they tend to give an overall picture of a society, for example. According to BAER et al., scenarios' goal is "to provide a self-consistent future world with a credible narrative leading to a plausible end point. Together, several scenarios span a space that is considered likely to contain the actual future state, although any individual scenario is by itself unlikely to be realized." [8]

It should be noted that many attributes that affect macro scenarios change slowly. Big ships do not turn fast and normally it takes time to make changes on a large scale. Furthermore, human behavior is largely coded in genes and therefore it is not expected to be revolutionized – the laws of physics seem to transform even slower.

The micro scenarios that I have analyzed above are possible in the time span of this thesis (see Time span, page 14). Before that, the technology is not developed

far enough. After that, the scenarios are probably outdated. Yet, that is quite short a time for macro scenarios. In about ten years the world at large will not change a lot unless an unexpected sudden catastrophe hits us. Surely, in the next decade, an upswing and a downswing in the economy will pass us, the world population will grow, pollution will increase, number of Internet connections and mobile appliances will raise, the divide between the rich and the poor will widen, and so on, but the overall picture will not change a lot. Especially, from the view point of this thesis, the new technical innovations will not have time to change the society dramatically. It takes years to make radical changes in laws, and the legal systems will not be very different after a ten-year period. The same business models that exist today will still prevail in the next decade. Therefore, in this thesis, it does not make sense to describe different macro scenarios to illustrate possible future societies. Instead, macro scenarios can be used to show the possible directions to which the society is going to develop.

In the following, I am briefly presenting several macro scenarios that others have developed. Then I conclude the most significant characteristics of them from this thesis' point of view.

Mobicom was an EU project (IST-1999-21000) that focused on fundamental factors that will affect the evolution of Mobile Commerce, such as market structure, key players, technology architectures, consumer behavior, new products and services. Mobicom created a set of macro scenarios, or Evolution Scenarios as the project called them, for Mobile Commerce services considering especially policy issues, market dynamics, methods of work, and business models. The four scenarios are summarized below. [1, 81, 82]

Mobicom Scenario 1: Business as usual – slow growth in search of business models. There has been a sloppy growth of mobile commerce, and the market constellation resembles the situation of today. The economic downturn and aftermath of the UMTS-licensing rounds have stagnated the anticipated growth.

Mobicom Scenario 2: Consensus of institutions for controlled growth. This scenario envisages an extended and well-developed value chain where service

providers, content providers and application developers have distinct roles as suppliers. However, the network provider, who controls the customer base, dominates the market. This is an ideal scenario from the operators' point of view. The big players control the development of infrastructure, standards, and services for mobile business. Thanks to industry-wide consensus, there are few or no problems in technology standards, privacy, IPR, etc. Some criticize this situation because large operators can raise entry barriers and limit competition.

Mobicom Scenario 3: Telecom is backing off. Telecom operators have agreed upon seamless roaming of mobile services all over Europe, as they see it in their interests to boost traffic on mobile networks. Competitively priced services are pushing operators back to the traditional telecom positions specializing in data transmission and maintaining the infrastructure. Importantly, customer billing may be carried out by any third party. Public investment in mobile services and effective regulation also foster a conducive environment. This has opened up possibilities for new entrants on the service market, notably third party service integrators. Consequently, consumers face a growing number of options for accessing the Internet, shopping, and paying over mobile networks.

Mobicom Scenario 4: Deregulated, liberalistic markets. Regulators have created and implemented a liberal mobile commerce policy, in order to boost competition on the common market. IPR-regulation is effective, and seamless services are provided over various networks. Last mile competition, portable subscriber addressing, transparent pricing of services has been introduced. The severe competition has boosted the innovation of services, however, few of them survive. Concerns remain in relation to the protection of personal information and related civil rights.

The Arizona Republic is an American newspaper. As many other conscious companies, it has also tried to discover its future operating environment by creating scenarios. Unlike most other companies, The Arizona Republic has also published its scenarios, and unlike many other scenarios, they are very well and carefully created. The three scenarios are characterized by terms *Steady Time*, *Real Time*, and *Zero Time*. The first of them presents slow change, technical problems, unhurried diffusion of

the Internet and e-commerce, difficult rollout of broadband, expensive wireless connections, strictly regulated privacy, and so on. The second is a moderate scenario. The third scenario portrays rapid change: seamless technology, inexpensive devices, unified standards, fast diffusion of the Internet, ubicomp, broadband access, wireless technologies, and e-commerce, privacy concerns are addressed through standards and technology, and so on. [116]

RAND Corporation has accomplished an interesting study, which principal goal was to build a broad framework for analyzing the relationships among ICTs, their likely economic and social consequences, and future energy requirements. They constructed a series of plausible scenarios for ICT growth and use from 2001 to 2021 through which to identify important driving factors and to distinguish likely trends and developments from those that are more speculative or highly uncertain. Although the main target was related to electricity requirements, the well-developed scenarios seem to be applicable more widely.

RAND's approach was interesting. They first developed one common scenario for the near future, i.e. year 2006, and then four other scenarios to which future paths may lead from the first scenario by year 2021.
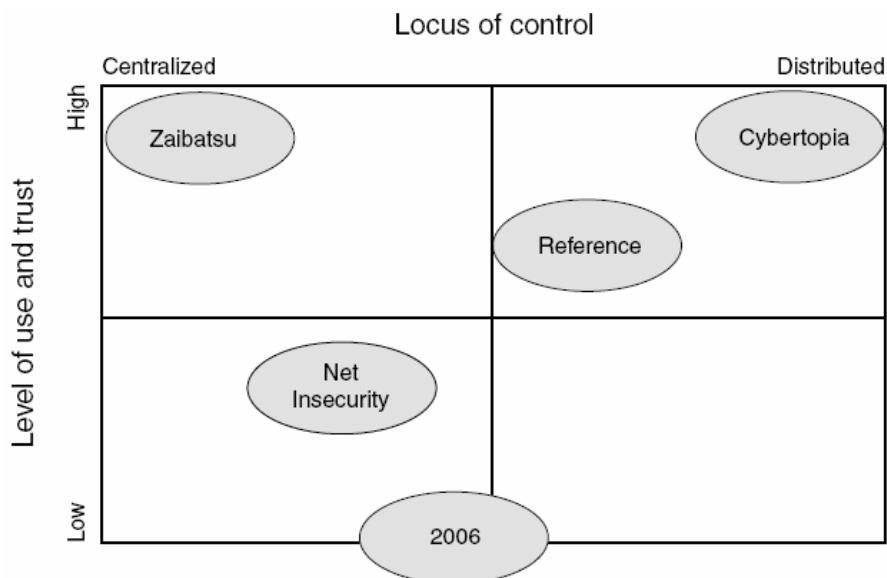

Figure 22. RAND Scenarios: Relationship of 2021 Scenarios to 2006 Base [8]

The four scenarios were called the Reference scenario, Zaibatsu, Cybertopia, and Net Insecurity. In their report, the developers of the scenarios carefully describe each scenario, the underlying presumptions, and conclusions. The *Reference* scenario essentially continues along the path of the first five years, moving steadily upward in usage and modestly toward further decentralization. *Zaibatsu* depicts higher ICT usage, with highly centralized control. *Cybertopia* shows ICT usage equally as high as that of Zaibatsu, but with control largely decentralized. *Net Insecurity* exhibits less overall ICT usage in 2021 compared to the other three, with more centralized than decentralized controls. [8]

Intelcity was an EU project (IST-2001-7373) that aimed at – among other issues – developing a range of visions and scenarios for future urban planning, design and city management through the innovative use of information and communication technologies. The efforts were seeking to predict role of ICTs in urban planning, design and management of sustainable cities by addressing the range of potential user needs (application pull) as well as new ICTs (technology push) for new e-working processes in the planning and management of sustainable cities. [91]

Intelcity developed 12 scenarios attempted to combine more sustainable urban forms and infrastructure which facilitate the knowledge society; and governance, planning and city management processes using ICTs to deliver more sustainable cities. Subsequently these had been integrated into five scenarios: e-Democracy City, Virtual City, Cultural City, Environmental City, and Post Catastrophe City.

Intelcity Scenario 1: e-Democracy City. In this scenario ICT is seen as an enabling mechanism, changing peoples' opinions and behavior patterns through information provision and empowerment. It provides new ways of decision-making and negotiation through inclusiveness and accessible participation in the decision-making processes that affect the community. This would involve the deployment of a variety of tools such as hard set accessible web based group decision support for visioning, advanced visualization tools, scenario planning and automatic translation as well as democratic participation tools such as e-voting and highly devolved decision-making. A peer-to-peer information system architecture is necessary, rather than

client/server, that would seek to provide educational support to enable understanding of the socio-economic and environmental impacts of various options under consideration in a way that dissolves boundaries, e.g. between interest groups and between physical and virtual worlds. The scenario is one in which self-determinism occurs within a socially cohesive community, respecting the wider community and the environment.

Intelcity Scenario 2: Virtual City. This scenario represents a knowledge society of networks and flows, where citizens are able to work and live anywhere in the city, supported by intelligent environments that are economically efficient and ecologically sound. Ubiquitous computing and telework lie at the centre of work and living. It also depends on the development of intelligent agents to provide of personalized, self-tailored information to support a culturally rich, mobile lifestyle. The scenario requires major infra-structural development in the supply of utilities and that both the economic and environmental transformation which this predicates would also require "strong" governance. This requirement however, provides the opportunity to use the ICT technologies both to empower citizens and make the corporate sector socially responsible. New social support groupings are established such as local virtual village halls as well as more dispersed partnerships (e.g. pressure groups) across the whole city and beyond. The scenario describes a more socially inclusive and therefore, progressive form of governance.

Intelcity Scenario3: Cultural City. This scenario expects a strong social and environmental ethic. It provides the ideal community environment where individual needs and well-being can be balanced with that of society in general. Advanced technology is present although entirely invisible - it is embedded. In the cultural city the additional means and channels of communication that ICTs provide assists, imperceptibly and unobtrusively, in all aspects of life. It is particularly useful in the negotiation and mediation necessary for agreeing collectively. At the heart of the city is a civic entity, space(s) for cultural and artistic exchange and democratic engagement. Thus it is framed and is facilitated by a fundamentally democratic decision-making process. This commences with commitment to stakeholder definition of goals and objectives for a new sustainable future and its delivery

146

according to a democratic expression of rights and responsibilities, individual, corporate and governmental.

Intelcity Scenario 4: Environment City. The scenario can be summed up as being of long life, low energy and adaptable. It is based on the realistic concept of incremental change in which all the current environmental and social problems are gradually addressed, solved or bettered over the period up to 2030. An important legal aspect supporting the scenario is the requirement on all manufacturers to recycle/reuse at end of life, thus closing liability loops, which in turn would reduce pollution to very low levels. In economic terms full employment would be stimulated through the adoption of a service economy where innovative means of extending product life would be sought. The value of "public goods" would be rediscovered. In social and cultural terms a multi-cultural, secure and safe society will be achieved through a combination of governance measures and the application of ICT. This would seek to increase 'self-organizing' capacities through better public information and participation in urban re/generation so that cities could become lively cultural places, which should tend to decrease current problems with crime and insecurity.

Intelcity Scenario 5: Post-Catastrophe City. The scenario is driven by albeit the small possibility of high impact events, such as a natural catastrophe, environmental catastrophe, or global war. This would considerably alter the relationship between citizens and the state and impact significantly on the freedom of choice of citizens. It is likely that wealth and quality of life would suffer initially with effective action being seen to be imperative in order to improve matters. Free market conditions would be unlikely to respond quickly or efficiently enough to events. Government would have to impose regulations to control behavior of markets, citizens and industry. Complexities and uncertainties in this situation are large. Means of encouraging rather than enforcing more sustainable behavior would be relevant. Amongst these uncertainties information and communication technologies would be highly relevant to such new forms of allocation of resources. It can enable real-time monitoring of resource use by individual citizens, companies and other organizations.

From the viewpoint of this thesis, the most interesting issue expressed in macro scenarios is the question whether governments and supranational regulators, like the European Union, will strictly control and regulate businesses, will some form of self-regulation increase, or will the markets, competition, and customer requirements chose the directions.

This is especially important issue in relation to privacy protection. At the moment, the European Union has chosen to regulate and control privacy and data protection quite intensively. Privacy is not considered to be a person's subjective right of which the person may dispose freely, but merely an area that is defined by law and protected by the society. Of course, people in Europe are still largely able to dispose on their private information. Most anything can be done with private information with the person's consent. Still, the current US approach is quite different: in America, the market-driven attitude allows people fairly freely decide whether they want to keep their private information secret, disclose it, or sell it – or ignore the whole issue. American laws do not ensure similar data protection as in Europe.

The most important differences between the European and the American approach become visible in cases which people ignore taking care of their private information: European law is more protective. Given that even privacy-concerned people often neglect protecting their private information, the European approach not to trust people's own ability to take care of their privacy is justified. [5] However, as discussed above, European data protection directives may disable scenarios that would otherwise be considered positive and providing interesting business opportunities and services for people. From that perspective, it is an important question for many companies whether lawmakers will apply more European or more American approach.

The macro scenarios present a number of non-legal challenges. For example, it will be important for any information product business model whether telecom operators will remain in a strong position or even strengthen their place in the markets, or will they merely provide infrastructure and sink away from information

products' marketplace. That however is hardly a legal challenge and resides outside the scope of the thesis.

LEGAL CHALLENGES AND MAJOR DISTINGUISHERS

Based on the scenarios analyzed above, I conclude that the legal areas including most challenges to information businesses will be

- privacy and data protection,
- intellectual property rights, and
- contracts.

Perhaps, the most important or at least very significant legal area will be *privacy and data protection.* Mobility, context-awareness, and ubiquity will bring computer networks even into the most intimate places and walks of life. As the scenarios show, future computing and communication devices are not only capable of accessing people's private information but many useful services are highly dependant on it. There will an increasing dilemma: people are requesting and can benefit from services that jeopardize their privacy.

Probably, the opposite interests of getting useful services and protecting privacy tend to seek balance. People are willing to disclose reasonable amount of private information to get the services they need, but not more than that. Certainly some people are more cautious of their privacy while some others do not care even if quite a lot of information on them is available for others. It certainly depends also a lot on the situation, social context, the services, and other factors, how much somebody is willing to disclose. Privacy is most relative. In a business meeting everybody is expected to introduce oneself while in an anonymous discussion group it is acceptable to use a pseudonym. Usually, it is at one's own discretion how much personal information she or he is willing to reveal.

On the other hand, for certain service providers there may be incentives to collect as much private information from people as they can, because that

information can be worth a lot of money. Also, as discussed above, it is often more difficult and expensive to build technical systems that secure private information than ignore privacy needs. Therefore service providers easily disregard privacy unless customers insist it or a legal system forces them to honor people's privacy.

The recent changes in legal systems, like European directives on data protection, have substantially improved privacy protection. Some of the chosen actions, however, make it difficult to develop services that users would like to have. For example, ISTAG *Maria* scenario above may turn out to be unfeasible, because it is difficult to implement the services in an efficient but legal way.

In summary, the opposite interests in privacy and useful services need to be balanced. The lawmakers must consider both sides and also understand what is technically feasible. Challenges to privacy are much greater than ever before.

It seems that *intellectual property rights*, particularly copyright, will be another legal area where a number of challenges come up. That is not surprising considering that the focus of the study is information products, and intellectual property rights often protect them. The interesting point, however, is that there seem to be emerging new kinds of challenges. Especially issues related to content adaptation will be significantly more challenging on the Mobile Internet than before.

On the other hand, although digital technology in general has made for example unauthorized copying easy, challenges related to copying, distribution and other fields of intellectual property rights do not necessarily change a lot from how they occur, say, on the wired Internet. Still, the increasing volume of certain subject matters will make even some well-known challenges more important. Challenges related to database protection for example will be more and more important because there will be rapidly increasing number of many kinds of databases on the Mobile Internet. Their legal significance will multiply even if there would not be any new challenges related to them. Similarly patents will be more important on the Mobile Internet because there will be many more patentable inventions, and trademarks will be increasingly important because of the growing importance of brands.

There will be major challenges related to *contracts*. First, on the Mobile Internet, it is not always easy to find out, who the contracting parties are. Second, it will be sometimes difficult to state what the subject of a contract is. It can also be complicated to determine when the parties have committed to the contract. Moreover, on a mobile network it can be troublesome to decide which is the correct law to govern a certain contract as well as which authorities have jurisdiction over disputes concerning it. Several scenarios above describe machines that make agreements on behalf of human beings or legal entities. This introduces severe challenges as discussed above.

Tax laws meet challenges because of new kinds of transactions, resources, and incomes as well as moving users, globalization, and changing work. According to FRYNAS, changing in future taxation of e-commerce are amongst the key policy risks facing Internet firms. Yet, the scenarios do not suggest that tax law would include significantly increasing challenges in the scope of this thesis. I agree that taxation is an important area, which should not be ignored in the strategic planning of information businesses. However, in the scope of this study, it does not look as important legal area as privacy, IPR, and contracts. [35]

There will be noteworthy challenges in other legal areas too. For example, international private law in general will be important, because of globalization and moving users. Administrative law can be challenged if administrative procedures are automated as for example ISTAG *Maria* scenario suggests. Labor law will face challenges because of changing work. Criminal law will be challenged not only by new kind of international and computerized criminals but also because it will be difficult to decide weather some objectionable act in the new environment is punishable according to the existing law. Constitutions can face challenges as political systems are challenged. Nevertheless, based on the scenario analysis, those other legal areas do not seem to bring forth as crucial challenges as the first three. In addition, legal areas like corporation law, environmental law, family law, procedures and litigation, property, and torts will hardly have new challenges to information businesses.

It depends profoundly on the viewpoint, which legal challenges are the most important. I have focused on four viewpoints, those of content provider, operator, device vendor, and user, because they represent satisfactorily different entities related to information businesses. The following table summarizes how much legal challenges I expect that there will occur in the legal areas from the viewpoints.

Table 3. Expected legal challenges in the legal areas from the viewpoints

	Content provider	**Operator**	**Device vendor**	**User**
Privacy	Numerous liability issues and constraints	Some liability issues and constraints	Support solutions	Numerous challenges
Intellectual Property Rights	Numerous vital challenges	Some liability issues, need to support solutions	Support solutions	Few challenges
Contracts	Numerous challenges	Numerous challenges	Support solutions	Numerous challenges
International private law	Some challenges	Some challenges	Support solutions	Some challenges
Labor law	Few challenges	Few challenges	Support solutions	Some challenges
Tax	Some challenges	Some challenges	Support solutions	Some challenges
Criminal law	Few challenges	Few challenges	Few challenges	Some challenges

Which are the most important characteristics or the major distinguishers of businesses that imply legal challenges? From the scenarios above, I have collected characteristics that cause the major challenges. They are listed in the table below.

152

Table 4. The major distinguishers of businesses implying legal challenges.

Business Distinguisher	Legal Challenge	Scenarios
Personal Information		
1. Service adapts in accordance with *context information*, like end-user's location or profile.	*Privacy*: data protection at large.	MobileIPR: 1 Between at large ISTAG: 1–4
2. Sharing products that may disclose *personal information*.	*Privacy*: data protection at large.	MobileIPR: 2 MC2: 1, 6 Between at large ISTAG: 1–4
3. Distributing pictures and other information on *famous people*.	*Privacy*: data protection at large but also *right of publicity* where applicable	MobileIPR: 2 Between 04-7
4. Processing *sensitive* private information (e.g. racial or ethnic origin, political opinions, beliefs, trade-union membership, and information on health or sex life).	*Privacy*: at large, especially rules on the processing of special categories of data.	MobileIPR: 2, 3 ISTAG: 1

Intellectual Property		
5. Need to *adapt information*.	*IPR* (esp. copyright): a right to modify information products and right in modified, derivative products.	MobileIPR: 1, 2 MC2: 2, 8 ISTAG: 1, 4
	Trademark law at large, esp. the owner of a trademark can forbid the use of trademark in connection with a modified product.	MobileIPR: 1 MC2: 2
6. Products include functionality, esp. *program code*.	*IPR*: Special provisions on computer programs may apply.	MC2: 1, 2, 4 Between ISTAG
7. The utilization of *large information sources*.	*IPR*: Database sui generis right at large, also copyright and other IPR.	MobileIPR: 1, 3 MC2: 1, 2, 4 ISTAG: 1
8. Users *sharing information* products with other users.	*IPR*: esp. copyright at large.	MobileIPR: 2 MC2: 1 Between 04-5 ISTAG: 1, 4

9. Utilization of pictures and other products that are made by *hobbyists* and *communities.*	*IPR*: esp. copyright moral rights, like right to be acknowledged to be the author.	MobileIPR: 2 MC2: 1 Between 04-7 ISTAG: 2, 4
10. Copying and superdistributing information products.	*IPR* esp. copyright and license terms.	MC2: 4 Between 04-5 ISTAG: 1
11. A new business method may infringe a patent.	*Patent law* at large.	MC2: 2
12. Using pictures that portray a person.	*Right in portraits*: a person may have a right to limit the usage of pictures that shows him or her.	MobileIPR: 2 MC2: 1 Between 04-7 ISTAG: 2
13. A service may transmit information that is not lawful.	*IPR*: *intermediate liability*, the applicability of *safe harbor* rules (esp. non-applicability, if the service does not fulfill all the *mere conduit* requirements, but for instance adapts or filters information).	MobileIPR: 1, 2 MC2: 1, 2, 8 Between 02-2 ISTAG: 1, 2, 4

Agreements		
14. In general, a *need to agree* on something over the network.	*Contracts* at large, but esp. the existence of binding agreements, the possibility to reliably identify contracting parties, and finding applicable laws and courts that have jurisdiction.	MobileIPR: 1, 2, 3 MC2: 6, 8 ISTAG: 1–4
15. Need to agree on rules with members of large *communities.*	*Contracts*: complex dynamic contractual relationships, management of numerous contracts, increasing transaction costs.	MobileIPR: 2 MC2: 8 ISTAG: 4
16. Need to *adapt content.*	*Contracts*: legally binding agreements with all parties on adaptation.	MobileIPR: 1, 2 ISTAG: 1, 4
17. Distributing pictures, video, or other information on *events,* or conversely trying to control event's information.	*Contracts*: esp. the existence of binding agreements between e.g. the organizers and the audience.	MobileIPR: 2 MC2: 1
18. New business models are incompatible with existing licenses or other agreements.	*Contracts*: the possibility to reinterpret or renegotiate a contract.	MC2: 8 ISTAG: 1

Other categories		
19. Users can access a service from *different countries.*	*International private law*: which laws apply, which courts have jurisdiction, where a judgment can be enforced. Esp. in *tax* law, which fisc has jurisdiction to tax.	MobileIPR: 1, 2, 3 MC2: 8 ISTAG: 1, 2
20. *Employees* in new working conditions and changing job descriptions.	*Labor law* at large.	MobileIPR: 2 MC2: 2 ISTAG: 1, 2
21. *New kind of transactions.*	*Tax law* at large.	MobileIPR: 2 ISTAG: 1, 2
22. *Public administrative processes* are automated or changed.	*Administrative law* at large.	MobileIPR: 3 ISTAG: 1–4
23. *Defect* in the system, *poor quality of service (QoS)*, or *incorrect information* that is provided may cause serious damage to others.	*Liability, torts,* and *damages* at large, esp. products liability. Liability for third party actions.	MobileIPR: 3 MC2: 1, 3 ISTAG: 3
24. *Games, lotteries and betting*: end-users may *win* something randomly or non-randomly, free of charge or on payment.	*Marketing law, consumer protection law,* and *special laws on lotteries and betting*: special regulations and prohibitions. If users abroad can access the service, which laws apply and which courts have jurisdiction?	MC2: 1, 7

25. A service leads users to *socially unacceptable behavior*	*Criminal law* and *ordinances* at large. The representative of the business might be liable for incitement if the users have been led to violate the law.	MC2: 4, 6

LEGAL IMPLICATIONS

DO NEW TECHNOLOGIES REQUIRE NEW LAWS?

Technological development tends to introduce new legal problems. Sometimes they can be solved using existing methods just by applying them in a new fashion. Sometimes the new legal problems need new kinds of solutions. Sometimes it is difficult to tell whether existing solutions apply or not. Some people are inclined to believe that most problems that come up with a new technology are totally new and that they need all new solutions, although – in practice – it would be possible to apply old rules to them. But some people also try to apply old rules to all the new problems refusing to see that some of the problems really need new solutions.

Recent advances in information technology have exposed both kinds of problems. For instance, machines are nowadays capable to perform some activities that previously were possible for human beings only. Therefore now, it might be a question about human-machine relationship where it used to be a human-human-relationship. Because of our very basic needs and beliefs, we want to rule human beings and machines differently. That is why those new relationships, to which machines are related instead of humans, may need different laws. The new technology also creates totally new phenomena. For example, hypertext or computer networks did not exist a few decades ago.

Often, new technologies also reveal artificial boundaries within laws. The recent development in software patents is a good example (see below). Or, it may appear that a law does not have a necessary boundary. For example, it might make sense to

limit the applicability of data protection law somehow (see below). These problems have been hidden until new technologies have made them visible.

The general idea to make laws as technology neutral as possible is indeed recommended, but hardly feasible in all cases. Below, I am giving a couple of examples on laws that unsuccessfully try to be technology neutral. At the end of the day, all the laws are based on some assumptions on the conditions in which they are to be applied, and if those conditions, e.g. technologies, change dramatically, the laws become unavoidably outdated.

PRIVACY IN INFORMATION BUSINESS

Most micro scenarios above present legal challenges related to privacy and data protection. Many of them are minor, but some of them are severe and could potentially prevent the avail of those scenarios in practice or turn them illegal. The frequent appearance of privacy issues in the scenarios implies the significance of this legal area for future information businesses.

Several factors affect the importance of privacy in the scope of this thesis. First, new technologies make privacy increasingly vulnerable. It is a fundamental property of many information and communication technologies that they need to manage information that can be related to individuals.

For example, the current telephone networks, both mobile and wired, are usually based on the assumption that the phone calls can be billed because the information on who called to whom is stored. That was not the case, when analog telephone exchanges did not store the detailed information but only the cumulative number of units how much phone calls had been placed from a certain subscriber connection. Nor is it the case in typical IP broadband connections, which usually have a monthly flat fee. Yet, the current model of storing detailed information on phone calls is such dominant – and provides such benefits – that it will not be replaced in the near future.

In the same way, to control access to computer and information systems usually requires information that can be related to specific individuals. It is technically possible to implement an access control system that does not need information that can be related to real individuals. However, the prevailing ways to implement access control systems do not make that difference. Likewise, certain technologies (e.g. broadcasting) make it easier to hide the fact what information certain person consumes, while other technologies (e.g. multicasting) by default let at least the sender know what somebody has received. Technologies can thus affect significantly how much information on individuals is available. Therefore, it is a technical necessity to manage personal information and limit its availability.

As computers, mobile phones, and other network devices proliferate and spread, they unavoidably get more information on individuals. Small ubicomp devices are not self-contained, but they are essentially parts of large networked systems. This means that they need to exchange information. Not all the devices can access to any information, but it is characteristic of the emerging information technologies that more than one device processes information. The challenges to data protection increase exponentially while the number of devices grows.

Second, private information can be used to improve and add value to information products and services. The scenarios above typically describe situations in which the end-users benefit from the fact that a product or a service can be adapted in accordance their personal circumstances. For example, Between and ISTAG scenarios at large represent such businesses. A context-aware service or a product that is adapted according to end-user profile can – at its best – provide end-users with exactly the service or information that is needed in a certain situation. While communication networks rapidly grow, the amount of available information or the information flood explodes. End-users are progressively more in need of technologies that filter away unnecessary noise and give them only the information they want. Therefore, the avail of personal information is not only sometimes acceptable, but increasingly necessary to let the end-users benefit from the possibilities that the information and communication technologies offer them.

Third, taking care of end-users privacy presents additional costs. Unless customers insist or laws require, it does not usually make sense for commercial companies to take measures to secure private information. Sometimes an entity may get competitive advantage by announcing that it follows a privacy policy, which protects end-users' information. Usually, though, individuals are not that concerned about their privacy that they would require companies to take the extra steps to protect it, nor get companies much advantage from voluntary privacy policies. Therefore, the laws of economics make the rational companies to ignore privacy protection as much as they legally can – or even as long as they don't get caught.

As discussed above, privacy and data protection law in Europe is quite strict and applicable widely. Usually, data protection law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. However, if a natural person, even for private purposes, puts personal data, like pictures on identifiable individuals, on a web page that is accessible by anybody, it is not considered purely personal and the law is applicable. As *Bodil Lindqvist* case showed, the one who creates such a web page may also commit a punishable crime. Therefore, any personal homepages or blogs that include pictures or names or other similar information on identifiable individuals without specific consent are illegal and criminal. There are probably millions of web pages like that – millions of people are committing such crimes all the time. [166]

There are other similar massive violations of data protection law. For example, any structured set of personal data, which are accessible according to specific criteria, is called a *personal data filing system* and it is governed by data protection law, unless it is for purely personal or household purposes. For example, each mobile phone and e-mail application includes an "address book", which is a structured set of personal data accessible according to specific criteria. If the phone or e-mail is used – even occasionally – for business purposes, the address book is a personal data filing system under the data protection law. In accordance with national implementations of data protection directive, all the personal data filing systems should be reported to national supervisory authority (in Finland *tietosuojavaltuutettu*) or a respective report (in the Finnish law, *rekisteriseloste*) should be kept available for anybody to see. There are

162

hundreds of millions of mobile phones, e-mail clients, and other applications that include personal data filing systems, but hardly any of them has been reported. The scenarios above suggest that the number of devices that include filing systems will increase remarkably. It means that the number of missing reports and thus violations against data protection law is also rising.

Do these massive violations of data protection law imply that people are evil or that the law should be changed? In a somewhat similar case, Electronic Frontier Foundation has argued that because so many people, about 60 million Americans, are breaking copyright law by sharing files over the Internet, the law needs to be changed. [175] On the other hand, many people are also driving too fast and walking through red lights, but it does not imply that traffic rules are not useful. Yet, these massive violations of data protection and copyright laws do imply that the laws are not quite up to the modern technologies and they should be revised. It is important to protect individuals' privacy and sometimes it can be insulting to publish a picture on a web page. However, if people in general do not consider it harmful to display pictures in public, why should it be illegal? Why should the law require a report on each mobile phone's address book, if nobody is making or asking them? Unlike copyright law, massive violations against data protection law are not prosecuted either. Neither authorities nor individuals are interested in them. So why not limit data protection law to cover only the situations that are actually meaningful for individuals, and make the law obeyable? Instead of announcing illegal all the web pages that include pictures of individuals, the law makers could choose another approach. Invasion of personal reputation is already a crime. If necessary, it could be supplemented with a notice-and-take-down procedure: a complainant serves a notice of infringing material to the entity that hosts the service, and the host removes the material to avoid sanctions. It is not in line with how people actually want to use the Internet to require a specific consent in advance in order to put any information related to identifiable individuals on the Net.

In conclusion, it is mostly up to lawmakers to find the right balance between privacy needs and the useful avail of personal information. As of now, they have not quite succeeded. In the European Union, the laws are too numerous and complex,

they cover unnecessary wide spectrum of information and circumstances, they include unnecessary provisions, and sometimes they may even harm useful businesses as shown above. If ISTAG Maria scenario is to represent a set of eligible future products and services, the laws should not prevent it as they seem to do today. On the other hand, in most countries data protection laws are too weak or even non-existing. To support the development of information and network society, a decent minimum level is required.

INTELLECTUAL PROPERTY RIGHTS IN SOFTWARE

The system of intellectual property rights was developed in quite a different world from the one we live in. Although human creativity and inventiveness have probably not changed a lot, new technologies and business possibilities have remarkably changed the environment in which the intellectual property rights operate.

Most information products nowadays are produced and used with help of computer programs. Many of them – especially multimedia products and games – even include programs. Copyright has been the most important legal tool to protect computer software, although until the 1980s, it was largely unclear if copyright protected computer programs. Many organizations were lobbying on behalf of *sui generis* protection. That is, they wanted to develop a special legal protection that would take care of the special characteristics of the computer programs. In the 1980s however, many legislators acknowledged that copyright should be the way to legally protect computer programs. In the U.S., the Copyright Act was amended to specify that computer programs are within copyrightable subject matter. In European Union, the Council adopted a directive according to which the member states protect computer programs by copyright, as literary works within the meaning of the Berne Convention. [76, 97, 134, 137, 155]

In recent years, many software companies especially in the USA have begun extensive patenting to gain a better strategic position among competitors. They are

now using patents as the primary means for legally protecting their software. In the 1980s and 1990s U.S. courts and USPTO gradually changed the rule. Therefore more and more inventions related to, for example, multimedia or Internet applications are within patentable subject matter.

This development has also been widely criticized. It seems that sometimes patents are issued too easily without proper examination. Also it is not clear in general that patents are the best way to promote inventions and industrial development. [e.g. 6, 76, 77, 110] In Europe, copyright has still kept its dominant position in contents and software industries, but also here, a lively discussion on software and Internet patents is going on. Despite the shortcomings, it seems obvious that patents are becoming increasingly important.

Most people probably agree that the valuable parts of computer programs should get adequate legal protection. The proper means to protect programs depend on what we believe is valuable in them, which is a difficult question to answer.

In their highly respected Manifesto, SAMUELSON, DAVIS, KAPOR, and REICHMAN discuss about intellectual property rights related to computer software. Although it was written several years ago, the Manifesto is still timely and addresses clearly the problems that are topical. They try to perceive among other things what makes a computer program valuable. Their arguments are strong and profound. However, a couple of questions presented in the Manifesto need some consideration. [113]

Samuelson et al are trying to reach the inner nature of computer programs by saying that "programs behave" and what is valuable in a program is not its textual representation but its behavior. The computer is a complex system. When we try to understand how the computer works, we need to simplify it somehow. It is often helpful, if we are able to kind of visualize it in mind in some way or another. However, there is a great danger that we oversimplify complex issues or that we left out something important from our picture. That may lead us to wrong results.

'Software' and 'program' are difficult and ambiguous concepts. For example, when we say that "we are using word processor program" we do not mean that we use the set of instructions or statements that form a program. We are not speaking of the computer system as a whole either, because we can run many programs in a computer at the same time. Instead we refer to an abstract machine, in this case to a kind of imaginary typewriter. For example, word processors usually implement a kind of paper metaphor: a white rectangle or "a sheet of paper" is displayed on the screen and black letters are "printed" on it. This creates an illusion that the user is actually writing on paper.

An end-user experiences a program mainly through a user-interface or through the functions that the program carries out. For such a user, it is quite natural to say that a program itself behaves. To define a program as an imaginary machine in this way is quite acceptable. However, it should be noted that this definition is different from the one above (see *Definitions* page 32). An imaginary machine is not a set of instructions or statements, but system behavior that a user experiences. A common mistake is to mix up these definitions and base an analysis on a wrong definition. If programs are sets of instructions or statements, they should be analyzed as such. On the other hand, if we referred to users' experiences and imaginary machines, it would be satisfactory to analyze their behavior, but the legal analysis of such concepts would make little sense.

The way a computer system normally works is that a processor reads program code, i.e. instructions one by one, and acts according to them. A program is usually quite a static set of instructions or statements. Albeit there are so-called self-modifying programs, the instructions do not usually change during the execution of the code. Instead, processing a program makes hardware act in a certain way, which in turn may change data in one way or another. Therefore, we should say "a program is a set of instructions or statements that make a system as a whole behave in a certain way" instead of saying that a program itself behaves. Thus programs are in fact merely text.

However, I do agree that behavior is valuable, not the text. Or, like MESSERSCHMITT and SZYPERSKI put it, "software informs a computer (rather than a person) by giving it instructions that determine its behavior. Whereas information embodies no behavior, the primary value of software is derived from the behavior it invokes; that is what it causes a computer to *do* on behalf of a user, and various aspects of how well it does those things." [78] Software is not valuable as such but as a part of a system. It could be compared to a steering wheel, which is not very valuable without a car, but which has a lot of value as a part of a vehicle.

Samuelson et al also compare programs to machines. I agree that software and machines have a lot in common. Especially, the complexity, the requirements of interoperability as well as building programs by assembling functional elements make software and machines similar. Nevertheless, it is hard to think that text is a medium of creation while in books, for example, text is the artifact created. To me, it is more logical to say that text is always an artifact that is created in a medium, whether the medium is paper, a disk, or electronic signals. The artifact, i.e. the text, then may cause something else to behave somehow. For instance, a book may cause me to laugh, a contract may cause me to fulfill my obligations, and a computer program may cause a computer system to process its input in a certain way.

As mentioned previously, useful articles are only seldom copyrightable. Computer programs are usually meant to be useful. Therefore one could expect that computer programs need to be especially creative in order to be copyrighted. However, this is not the case. In many countries, the level of creativity needed to copyright a computer program is especially low. [40] To me, this is only illustrating the fact that there is something fundamentally wrong in the legal protection of computer programs and that the current solutions – copyright, patent, and so on – do not easily fit to programs but they need to be compelled to give protection.

For years, there has been a lively discussion about the patentability of computer programs. Previously, programs were likened to mathematical methods, mental acts or games, and thus not patentable. Case by case, these limitations have crumbled away. The United States has led the development, but the rest of the world is

following. The United States Supreme Court had decided in 1972 that programs are not patentable [163]. However, often cited as a US landmark case, *In re Alappat* [164] effectively brought programs into the field of patentable subject matter. In 1998 the Federal Circuit unambiguously permitted patents on "pure" software. [76] Moreover, U.S. Patent and Trademark Office (USPTO) has begun to issue Internet business method patents [e.g. 159, 160, 161]. In my opinion, it was not that much of a policy change, but the realization of the fact that none of the artificial boundaries that were supposed to prevent patenting programs were actually justified. It was realized that computer programs are not that different from machines and other patentable subject matter. The logical conclusion was that programs must be patentable with the same prerequisites as other inventions. The development went even further: in *State Street Bank* [167] court found that business methods are also patentable. This caused a huge boom of patenting business methods related to electronic commerce. The European countries have followed the USA. Although the European Patents Convention (EPC) still states that programs *as such* are not patentable inventions, in practice computer programs are largely patentable in Europe and discussion about patenting business methods is lively. Similar development is ongoing around the world. [41, 48, 62, 69, 76, 77, 114, 121]

To me, this is not the end. The current boundaries of patentable subject matter will also be found artificial and the area will extend and extend. It seems that any natural borders cannot be found. Of course, lawmakers can build statutory limits and declare that nothing outside this area is patentable.

This however is not satisfying if the boundaries are in more or less arbitrary positions. On the other hand, if the development may continue, the patent system will eventually collapse. To avoid these problems, whole the patent system should be revised. The new technologies have introduced new kind of inventions. It is an important policy issue to go through the fundamentals of the patent system and see if more than a century old primaries should be reconsidered.

The main shape of legal protection for information technology is nowadays fairly clear. Copyright is protecting software and contents. Most entities do not think

it is acceptable in general to make copies of programs and other works without permission. Patents protect hardware as well as innovative processes and structures in programs. [41, 48, 62, 69, 76]

Open source software development is gaining more popularity. It challenges traditional ideas on how strong intellectual property rights promote development. The supporters of open software movement do not want to restrict the copying and modifying their programs. They are still willing to develop software although anybody can copy, change and use it freely. Open source development is based on strong legal rights that are licensed in a liberal and allowing manner. Even if one does not believe that the open source model will dominate in the future, it certainly shows that strong protection is not the only way to solve the legal questions about software. [132]

I conclude that copyright is actually a reasonable way to protect the textual parts of a computer system, i.e. programs. Then again, the real value of a system is not in the text but in the behavior that is not protected by copyright. This in turn leads us to think if – for example – patents would be a better means to protect the real valuable parts of computer systems.

Having said that, I am not endorsing the current practice of patenting everything. Instead, I suggest that ideally a better system should be developed considering what is actually valuable and worth protecting. Maybe software legal protection could benefit from a similar sui generis right that is now protecting databases in Europe. After all, many computer programs do not include such novel and non-obvious ideas that they would earn patent protection. And even if a part of a program is patentable, the rest of the program remains unprotected. Instead, it is often laborious to build a useful program and therefore legal protection for investments - like the database sui generis right – might be the best way to protect what is actually valuable. I do understand that developing a new international legal protection system is not an easy or a quick job. However, the current system has so many flaws that sooner or later it should be fixed.

INTELLECTUAL PROPERTY RIGHTS IN DATABASES

It should be noted that the word *database* is ambiguous. Especially, a 'database' in information technology and a 'database' in legal context are not necessarily the same. According to the database directive, the term 'database' means a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Databases should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data. This means that a recording or an audiovisual, cinematographic, literary or musical work as such is not a database. On the other hand, not all the databases that fulfill this definition gain database protection. It is namely further required that in order to get the *sui generis* right in a database, it must show that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents. [95, 131, 141]

In addition, "works, data or other material" in the definition of database are quite troublesome. Obviously the directive is trying to state that databases can include many kinds of information, copyrighted works as well as other sets of information. The wording, however, is quite unsuccessful. 'Data' here do not refer to methods of recording as defined above, but rather to information. 'Material' on the other hand probably refers to *im*material items. Therefore this part of the definition does not help us much. [95]

All the EU member countries need to have implemented the directive. However, they have had the liberty to implement it in their own ways. Therefore the database legislation differs slightly within the European Union. For example, in the United Kingdom, the legislator has chosen to include the definition of a database in the statute quite directly from the EU directive: "'database' means a collection of independent works, data or other materials which (a) are arranged in a systematic or methodical way, and (b) are individually accessible by electronic or other means" and a "property right ('database right') subsists […] in a database if there has been a substantial investment in obtaining, verifying or presenting the contents of the

database." [138] In Finland, on the other hand, the legislator has chosen not to specifically define *database* in the statute, but to declare only that the sui generis right requires a substantial investment in obtaining, verifying or presenting the contents of the database. [153]

So, what is a database? From the technical point of view, a database system in a computer consists of several components. There is a collection of data and a collection of programs to access the data. According to KORTH and SILBERSCHATZ, a major purpose of a database system is to provide users with an abstract view of the data. That is, the system hides certain details of how the data is stored and maintained. [66]

This is accomplished by defining three levels of abstraction at which the database may be viewed: the physical level, the conceptual or logical level, and the view level. Physical level describes how a record is stored. Logical level describes data stored in database, and the relationships among the data. On view level, application programs hide details of data types. Views can hide information for security purposes. There can be different views for each user based on for example users' needs, rights, and security requirements. [66]

It seems that many database systems perform this task in such an excellent way that most users cannot make distinction between the three levels of abstraction. Instead they think that the view they see is the actual database. Unfortunately, the legislators do not seem to be able to avoid that confusion. This makes the legal analysis quite difficult. What is the subject matter of the database protection? Is it the view a user sees or the actual data stored on the physical level or something in between?
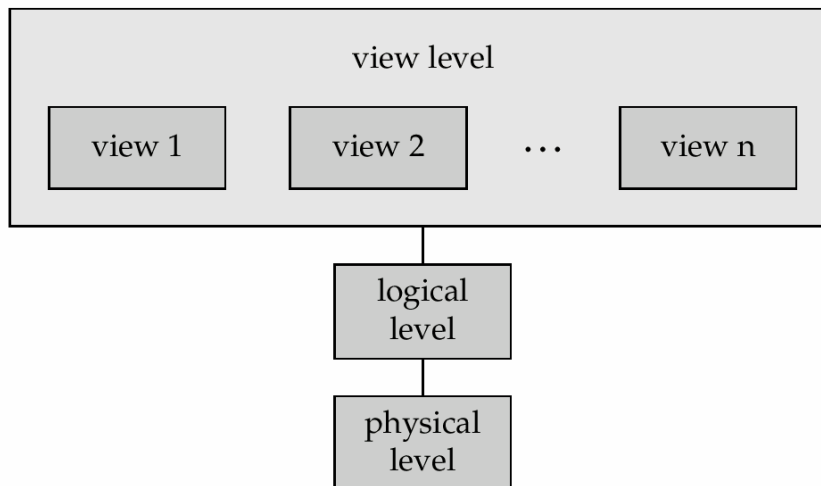
Figure 23. The three levels of a database system. [66]

Let us get back to the legal definition of 'database' in the directive: a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. I am mostly concerned about the requirement of systematic or methodical arrangement. Let us consider an example. Suppose a group of biologists makes a detailed catalog of natural resources of wildlife and game in a particular area. It takes months to collect, store, and verify the data. The outcome is valuable as the inventory can be used in many studies. However, I find it hard to describe such a list of natural resources "arranged in a systematic or methodical way". To be valuable, the list does not need to be even in alphabetical order. It can be just the Latin names of species in a random order but a user can still analyze the information with a computer. Is that a systematic or methodical way? Hardly. If the sui generis right requires more than trivial arrangement of data then valuable lists – even if they have needed substantial investments – do not gain the right.

In a computer-based system, databases are typically arranged by attaching an index to them. For example, data items can be stored into a database in whatever order they arrive, but a constantly updated index is used to keep the data items in order. This can be done fully automatically so that a user does not see indices and the indexing process at all. The actual data can be completely unarranged. Yet, a user can

make queries and the database system software shows results arranged as the user wants. This representation does not necessarily have anything to do with the actual arrangement or unarrangement of data in the database. An index is meant to increase the performance of a database system so that frequent queries can be completed rapidly.

However, indices are usually not mandatory. A database system can be fully functional, only somewhat slower, without indices. The same queries can be carried out by the system with or without indices. Usually, there is no use to optimize infrequent queries using indices, but it is still possible to carry them out. If there are no indices or no index is useful for a certain query, the system must at worst go through each data item to decide whether it matches the query. This takes computing power and time, but it does not affect the results.

For example, it could be possible to display all the Latin names of the species in an inventory that include letter 'u' and sort them in the alphabetical order. The outcome would look like the data in the database were in order or at least properly indexed, but in fact it does not tell anything about the arrangement. A similar outcome can be displayed even if the database is completely unarranged using only computer's brute force to complete the query.

What is valuable in databases? What need to be protected? Certainly individual data items can be valuable, but as discussed earlier, they should not be protected as such in general. Instead, it can make a lot of sense to protect large investments that are needed to obtain, to verify, and to present the contents of the database. The sui generis right should be seen as a legal protection of certain large investments. From this point of view, the arrangement of a database is not essential; it does not necessarily need to be included in the definition of 'database', although a significant investment in arranging data can help to achieve the sui generis right.

The requirement that the data items are individually accessible is also problematic. It seems to refer to that the items in the database are distinct in a way that they can be found and accessed independent from others. However, there is a difference what in principle would be possible for a computer program to find and

access on the database system level and what in practice is possible for a user based on the decisions that the database designer has made.

From the legal point of view, it would make sense to emphasize the user view point, but then the sui generis right would depend quite randomly on – for example – usability or security requirements. Typically it is neither possible nor reasonable to give users access to all individual data items.

Nordic countries, Finland, Denmark, Iceland, Norway, and Sweden, have also another neighboring right called *catalogue right*. According to Finnish Copyright Act, a catalog, table or program, or any other production in which a large quantity of data are compiled, shall not be reproduced without the consent of the producer. A program in this context does not mean a computer program, but more like a schedule of activities. The catalogue right does not require that data are arranged in a certain way or that data items are individually accessible. The only requirement is that the quantity of compiled data is large. This approach seems to avoid many problems described above, but – as mentioned – the catalogue right is available only in a few countries. Also, the catalogue right does not require investment. Therefore, it is arguably sometimes too easy to get the catalogue right. A better solution might be a kind of combination of database sui generis right and catalogue right, that is, a sui generis right that requires investment, but does not define database too strictly. [41, 62, 153]

To conclude, the definition of 'database' in the directive is questionable. It is hard to tell on which level of abstraction both arrangement and individual access refer to. Therefore they should not be given noteworthy meaning. Instead, the requirement of significant investment is important. Parallel to originality, novelty and non-obviousness, distinctiveness, and so on, it adds a vital new area of subject matter into the field of intellectual properties. [95, 131]

In Figure 2 above, I have illustrated how the levels of abstraction related to intangible objects affect legal protection. The question arises, does database protection fit into the picture and on which level it would be. Obviously, the database sui generis right has a significant extra dimension – investment – that is not

shown in the Figure 2. Therefore the sui generis right may protect databases on the several levels of abstraction. However, we can still exclude some of the levels.

The database sui generis right does not protect physical medium. If an appliance that is used to store a database is stolen, the thief does not infringe the database right, but violates the ownership.

How about data? Does the database right protect the bits or the representation in a binary form? No, it does not. Suppose one has a protected database in an IBM mainframe system. If the database is transferred into a UNIX or an MS Windows system, it is possible that the binary representation needs to be changed. For example, letter x in IBM's EBCDIC code is represented as the binary string *10100111* while in ASCII code, x is *01111000*. The indices are probably regenerated. It is possible that most bits are changed while transferring a database from one system to another. Yet, the database right remains untouched – both the original database and the transferred version are protected alike, or from the database right view point, the two databases are the same. Therefore, the database right is not related to data either.

Instead, it is related to information. That is, the contents of a protected database need to have some meaning. On the other hand, the database right does not protect the information or the meaning itself but – as described earlier – the large investments that are needed to obtain, to verify, and to present the information.

The sui generis right provides the maker of a database with the right to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. [141] Although individual data items in a database are not protected by the sui generis right, not only the database as a whole is protected but also a substantial part thereof.

What is a substantial part? As suggested above, the most important qualification for the sui generis right is significant investment. Therefore, to judge what is substantial, the amount of investment should again be considered. If the investment needed to make a part of a database is significant, that is, if the part alone could be

considered to gain the sui generis protection in case it were a separate database, then the part is a substantial part and its extraction and re-utilization without consent is prohibited.

So, the sui generis database right requires substantial investment. The investment must be in obtaining, verifying or presenting the contents of the database. If the investment is aimed at something else, it does not constitute the database right. This is illustrated by *spin-off* doctrine that is especially popular in some courts in the Netherlands. For example, a television program listing, a real-estate listing, and a headlines listing were not databases according to Dutch courts, but merely spin-off products of other activities. On the other hand, Dutch courts have several times held that telephone catalogues and subscriber data are databases. [50, 131] The logic here is not quite clear: it seems that telephone catalogues and subscriber data do require investments, but they are mainly outcome of other activities, namely marketing, customer recruitment, customer service, and the necessary information collection. How large a part of the investment is accomplished just for the catalogues? Probably usually quite small although it is obviously possible to develop a database on subscriber information that needs a lot of investments. As suggested above, the database sui generis right should protect specifically investments in databases. Therefore, it does not make sense to count investments in other activities. Therefore the spin-off doctrine in general is acceptable.

INTELLECTUAL PROPERTY RIGHTS IN METADATA

In general, intellectual property rights protect the content of an information product and related computer programs. On the other hand, the metadata of an information product is usually not protected. By and large, metadata consists of facts, definitions, identifiers, and so on. If it is organized in an original way, metadata might be copyrightable as a whole, or if metadata includes, for example, creative expressions like descriptions of content or summaries of it, then that can be copyrighted, but usually information items within metadata are not copyrightable. Typically, but not without exceptions, there have not been such substantial

investments in metadata that would entitle to the database right. Especially methods of processing metadata can be patentable, but not metadata itself.

In some cases, however, parts of metadata can be legally protected. For example, based on Article 12 of the WIPO Copyright Treaty [158], many countries have changed their copyright laws so that it is now illegal "to remove or alter any electronic rights management information without authority". Trademarks can also protect parts of metadata and, arguably, some metadata could be claimed as trade secrets.

CONTRACTS ON INFORMATION BUSINESSES

HUGENHOLTZ claims that "prima facie, contract law has all the makings of a perfect alternative to copyright protection. The structure of the Internet facilitates the establishment of a multitude of contractual relationships between information producers and end users, either directly or through intermediaries. The Internet (or more precisely, the World Wide Web) is uniquely suited for this purpose. Both its 'textual' environment and its interactive nature are ideal conditions for a contractual culture to grow and flourish. Contract law, thus, may become the instrument par excellence to fill the legal vacuum of the Internet. Information producers, intermediaries and end users are free to create their own rules, without government intervention, and to experiment at will with novel legal approaches. Ideally, new legal norms may emerge from this self-regulatory laboratory; norms far better tailored to the new environment of the Internet." [48]

HUGENHOLTZ lists a number of doubts about Internet contracts. He is afraid that weaker parties risk being subjugated and fundamental freedoms may be jeopardised if most relations are governed by contracts, not laws. He also raises question about validity of so called 'click-through', 'mouse-click' or 'click-wrap' contracts. [48]

Further, HUGENHOLTZ asks whether the terms of user licenses can override the statutory limitations of copyright. [48] Actually, it may be difficult to get round

mandatory laws using contracts, but many rules are not mandatory and there are many potential claims and relations that laws do not say anything. It seems quite clear that it is largely possible to extend intellectual property rights in contract terms. For instance, in a license agreement, a licensor and a licensee can agree that the licensor has rights that are not stated in the law. That kind of an agreement is normally binding and enforceable between the contracting parties. It seems that these agreed intellectual property rights are becoming quite common and significant. [112]

The word *contract* may refer to several different concepts. In legal language, a *contract* is an agreement between two or more parties creating obligations that are enforceable at law. Often *contract* also refers to a specific document, a writing that sets forth such an agreement. [36] From the legal point of view, it is fundamental that a contract is a declaration of intention: it expresses contracting parties' will. The freedom of contract principle states that contract is legally binding in whichever form as long as the parties have wanted it, as long as it corresponds their will.

From a technical perspective, especially in relation to digital rights management, *contract* may refer to a document that includes formal, machine-interpretable expression of permissions that one party gives to another with respect to certain information product. The computer system may then be able to enforce the permissions and especially their restrictions.

It is noteworthy that the set of legal contracts and the set of DRM contracts are overlapping but not the same. The intersection of those two sets includes contracts that are legally binding and fulfill the formal requirements of a DRM system. The intersection is not empty because it is perfectly possible to write such contracts: according to the freedom of contracts principle a DRM contract may be legally binding, if it corresponds to the intention of the contracting parties. And a legally binding contract can be a DRM document as long as it is written in a formal rights expression language (REL). However, typically a legally binding contract is not written in REL, thus most legal contracts are not DRM contracts. Also, many DRM contracts are not legally binding and therefore not legal contracts.

Also, a legal contract typically covers whole the legal *contractual relationship.* Together with applicable laws, it defines all the rights and duties of the parties with respect to certain subject matter. A DRM contract, in contrast, typically covers only a subset of rights and duties of the contractual relationship – namely those that a machine is able to control. An interesting question is how large a part of all the rights and duties in contractual relationships could be covered by DRM contracts.

Not only the word "contract", but also other terminology is different between digital rights management and jurisprudence. For example, in a DRM system, an end-user is typically granted permissions such as *display, print, play, execute, modify, excerpt, annotate, aggregate, sell, lend, give, lease, move, duplicate, delete, verify, backup, restore, save, install,* or *uninstall,* which are functional operations to an *asset.* [90] In a legal system, on the other hand, an end-user can have rights such as *reproduction, public performance, recordings, broadcasting, translation,* or *adaptation* in a *work.* Mapping between DRM terminology and legal terminology is not straightforward. The ambiguity becomes even more challenging, when the dynamical characteristics of legal language are considered: legal terms have different meaning in different contexts, jurisdictions, and times.

From the legal point of view, a contractual relationship – e.g. between a content provider or licensor and an end-user or a licensee – is governed by the terms and conditions of the contract – in this example, the license agreement – and the provisions defined by law. Should a DRM system be able to control whole the contractual relationship, it needs to have information on both the terms and conditions of the agreement as well as provisions in law. This information can be transferred to the system by the technical DRM contract, or it could be imagined that the system knew the rules of the governing legal system otherwise and needs to get only the terms and conditions of the agreement per contractual relationship.

In practice, considering the dynamical nature of legal systems, and different characteristics and contexts of each contractual relationship, it is hardly possible to assume that the DRM system has enough information on the governing legal system. Therefore it makes more sense to include the necessary legal provisions in the DRM contract, if the DRM system should govern whole the contractual relationship.

Obviously, the other alternative is to decide that the DRM system does not control the contractual relationship as a whole but only a subset of it. In that case, the interesting question would be how to define the subset. For example, would it make sense to control only some terms and conditions if a party is able to violate the rest of the provisions? The profound question is which parts of a contractual relationship should be governed by a DRM system and which parts are left for the judicature.

Some interesting situations may come up because of new legislation. For example, the Finnish Copyright Act includes a provision that would force content providers to let non-profit libraries to make certain copies, e.g. backup copies, even if the content is copy-protected. A perfect DRM system would be able to allow this kind of copying despite the terms and conditions in the contract. [153]

So far, electronic contracts have only a little tradition. The huge body of statutes, case-law, and legal tradition govern the interpretation of conventional contracts. Each law student can tell when a contract is binding. Therefore risks involved in traditional contracts are limited and manageable. However, as of now, electronic contracts involve a lot more severe risks. New laws and the new European directives are improving the situation (e.g. the Directive on electronic signatures and the Directive on electronic commerce). Yet, until the field is well enough established an entity takes more risks if it makes electronic agreements than making conventional contracts. [35, 67, 143, 144]

It should be noted that certain types of contracts cannot be in an electronic form. For example, in Finland the sale of real estate must meet the requirements in form prescribed in law. An electronic contract cannot fulfill those requirements and thus the sale of real estate cannot be accomplished completely electronically. That would be an absolute obstacle for a business model that was based on an idea to make electronic sales of real estate. [67, 143, 144]

In some cases it is, in principle, possible to make contracts in an electronic form, but in practice the form prescribed by law is too strict to be fulfilled. [67]

An important characteristic of a contract is its *unfalsifiability*. Conventional paper documents have plenty of strength of evidence, because they are not easy to forge. Technologies to be used in connection with electronic agreements should not undermine the probative force of the contracts. Mobile technologies do not necessarily endanger the unfalsifiability of the contracts; on the contrary, empowered by strong cryptography and digital signature technologies they may enable even greater security. [67, 143]

Yet, it is often possible to replace conventional contracts with electronic agreements. At its best, instead of awkward long-term paper-contracts, a company could flexibly call for competition subcontractors and make electronic agreements separately on each transaction. Traditionally each contract represents additional transaction costs, which makes it more profitable to use fewer contracts that cover long-term relationships. If computerized systems are able to make agreements automatically with small transaction costs, it would often be beneficial to use numerous short-term contracts or make separate agreement for each transaction. However, as yet, electronic agreements present more risks. Conventional agreements involve smaller risks because they are well-established and better known. Therefore, many companies that are aware of legal risks hesitate to use electronic agreements and tend to stay with the old, less flexible business models. [35, 94]

In an electronic market place, buyers and sellers can agree flexibly on each transaction. If however, companies are worried about uncertainties related to the electronic form of contracts, they are willing to stay with old well-known formats. In other words, they are not ready to exploit new technologies.

A compromise between conventional and electronic contracts can be an arrangement in which parties make a *skeleton agreement* in paper. It regulates the contractual relationship in general and specifies how electronic agreements bind the parties. For each transaction thereon it is relatively safe to make agreements in electronic form.

Obviously that complex an arrangement is not always possible. Especially, it does not enable an entity to choose the other party freely like electronic contracts

might do, but the company needs to stay with the companies with which it has skeleton agreements.

Electronic agreements make most sense in B2B relationships when they can be automated. For example, if a manufacturer needs to order parts from a subcontractor and the number of transactions is large, it is beneficial if the manufacturer's computerized inventory management system is able to send orders automatically to the subcontractor's delivery system. The subcontractor's system in turn sends an acknowledgement and confirms the details of the delivery. If something needs to be changed, the two systems can again send messages and agree on the new conditions. The messages those systems send and receive could form binding contracts. That however requires at least two things:

1. From the legal point of view, the messages must represent the will of the companies and form a mutual understanding between them. In general, agreements between computer systems are problematic as computers in general cannot legally represent companies. Often, it is possible to remove that obstacle by a skeleton agreement arrangement described above.

2. From the technical point of view, it is not enough that the systems can send messages to each other. Even a general set of common specifications, like ebXML (Electronic Business using eXtensible Markup Language), is not enough. The two systems must have the same ontology, that is, they have to share the same understanding of concepts. If the systems do not have a common language to describe, for example, what is the object of purchase, it is impossible to make an agreement. The new technological advances and common standards (e.g. RosettaNet, http://www.rosettanet.org/) are reducing these problems.

In conclusion, the readiness to use electronic agreements between computer systems usually requires that the entities have agreed in advance on the legal status of the messages that the systems send to each other as well as on the communications standards, the protocols, the languages and the concepts they use. [94]

Flexibility is one of the key issues related to mobile technologies. In relation to contracts, it means that the companies should be able to flexibly change their commitments in mutual understanding.

In relation to wireless technologies, there are new kinds of contractual challenges. For instance, while users are moving, they have many kinds of wireless devices, and their access points keep changing, it can be evermore difficult to identify who the user is. From the contractual viewpoint it is troublesome if the other contracting party is not able to be sure who the other party is. This can be helped using for example digital signatures that are certified by a trusted third party. However, that requires technological solutions that may be restricted by the readiness of the companies. [98]

CONCLUSIONS

My first goal in this thesis was to demonstrate how to study future legal challenges. I have developed a scenario-based method that produces lists of legal challenges and helps to analyze them. From the methodological point of view, I have demonstrated the usefulness of scenario generation and analysis in legal research. It differs significantly from the currently prevailing paradigm of legal science. Especially, the method does not honor the doctrine of sources of law, which is fundamental to jurisprudence. Therefore my study cannot be called legal science, or at least not legal dogmatics. Yet, I believe that adopting such new ways of thinking and analysis will be important to keep legal studies useful.

The method highlights products and services. Other business aspects are paid less attention. Also, specific characteristics and organizational cultures of particular companies cannot be considered in a general method like this. Therefore certain legal challenges remain largely unnoticed. It seems that the method is able to point out numerous relevant legal challenges – especially those that are *directly* related to products and services. For example, challenges related to products and services that will possibly infringe privacy or intellectual property rights are easily visible. On the other hand, challenges that are *not directly* related to products and services, but more to – for instance – a company's position in the marketplace, remain mostly hidden. Therefore challenges in legal areas such as competition law and corporate and financial law do not appear in this study although in practice they can be relevant. In the future work, it should be studied whether it is possible to extend the method to cover these areas also.

Typically, micro scenarios, like those analyzed in this study, do not describe business models and revenue logics. Therefore, legal challenges that are related to business models remain largely hidden. Especially issues concerning tax law, competition and anti-trust law, and corporate law are difficult to point out with this kind of scenarios. This seems to be an important shortcoming of the method.

In general, the study does not expose all the legal challenges. Even within the scope that I have defined in the beginning of the thesis, there can be legal challenges that cannot be found using this method. However, the method is useful, if it reveals significant new legal challenges that were otherwise left unnoticed, or if it provides an easier and a more systematic way to find the challenges. It remains to future work to extend the method to cover also the rest of the legal challenges. Therefore, the method in its current form has significant limitations, but taken them into account, it still produces valuable output.

Legal rules can affect businesses in many ways. At their best, they enable businesses, but too often they also harm useful activities. I conclude from the analyses above that the following business drivers are important from the legal point of view:

- *Balanced legal rights.* For example, privacy needs to be protected, but data protection must not prevent useful business; reasonable consumer protection enables, not harms, B2C business. They ensure the interests that will enable consumers to shop with confidence and thus increase the commerce.
- *Anticipated outcome of legal processes.* Understandable, unambiguous, and easily applicable laws diminish uncertainty and risks related to future operations.
- *Up to date rules to minimize transaction costs.* Laws that are up to date and cover a case in question, decrease the need to draft contracts case by case, and thus they reduce transaction costs.
- *Fair allocation of intellectual property.* It encourages both to produce and to consume information goods, if rights in them are allocated in a fair way.

On the other hand, the following legal hurdles are also important:

- *Unbalanced legal rights.* Too strong or weak privacy protection, unbalanced consumer protection, unfair allocation of intellectual property rights, and so on, cause social problems, slow down economic growth, and hinder businesses that depend on those rights.

- *Outdated laws are difficult to apply.* Old laws in the new context make legal decisions unexpected and random. Outdated laws create also barriers to entry the markets with new technologies.

- *Technology-biased laws introduce extra costs.* Despite good will, it is impossible to make laws completely technology neutral. More biased they are towards certain solutions, more difficult it is to entry markets with different technologies.

- *Unclear legal status of new communities* slows down the pace people can avail of them.

In this study, I have pointed out the areas in which legal challenges plausibly arise. Would it be possible to actually *analyze the legal risks* related to future businesses? What are the actual legal risks related to a certain future business, how *probable* they are and what are the *expected losses* if they occur? Details in legal systems vary by time and by jurisdiction. Therefore, on a general level, analysis cannot go into legal details. However, as the saying goes, the devil is in the details – they may often be crucial. The approach is not useful if the details are ignored completely. For example, let us suppose that a company is considering a business idea that would bring the company in between a content provider and an end-user. One of the legal questions in that case would be whether the company was an intermediary that is liable for copyright infringements. The main principle is that if a service provider distributes information that infringes someone's copyright, the service provider can be liable. However, the safe-harbor rule in copyright law immunizes the service provider if it is a *mere conduit.* Yet, the rule does not exist everywhere, and it depends on the details of the definition of "mere conduit" when it is applicable. The actual result, whether there is a legal challenge or not and how severe it is, may thus be very sensitive to the details of the legal system. Consequently, a more precise risk analysis requires detailed information on the case in question and it is not feasible on a general level. In the

future work, however, it would make sense to study how to assess the legal risks more in detail in a certain case.

In this study, the legal systems are considered rather static. I have not studied extensively, how the legal challenges will change, if the legal systems transform. Considering that the time span in this study does not reach farther than a decade and that the legal systems do not change rapidly, the presumption is probably not grave. However, in the future work, the dynamic nature of legal systems should be taken into consideration.

I have listed, analyzed, and discussed the future legal challenges that I was able to point out using the method. I conclude that the most important legal challenges to future information businesses are within the areas of

- privacy and data protection;
- intellectual property rights; and
- contracts.

I have also discussed above the major distinguishers of businesses implying legal challenges. They help to indicate the specific legal challenges related to a certain information product or service.

TABLES OF FIGURES AND TABLES

FIGURES

TABLES

REFERENCES

BOOKS AND ARTICLES

1. A. Aarnio, A. Enkenberg, J. Heikkilä, S. Hirvola. Scenarios for Mobile Commerce in 2006, Report D.5.1 in MobiCom European Fifth Framework Project IST-1999-21000. In *Evolution Scenarios for emerging M-Commerce services: New Policy, Market Dynamics, Methods of Work and Business Models*, the Mobicom Consortium, Ioanna Constantiou, ELTRUN - the eBUSINESS Center, Athens University of Economics and Business (AUEB), 2002.

2. A. Aarnio. *Lain tulkinnan teoria.* (In Finnish.) WSOY, 1989.

3. A. Aarnio. *Uusi varallisuusoikeus – vai vanha?* (In Finnish.) Lakimies 4/2002.

4. K. Aberer, M. Punceva, M. Hauswirth, R. Schmidt. *Improving Data Access in P2P Systems.* IEEE Internet Computing Vol. 6, no 1, January/February 2002.

5. A. Acquisti, J. Grossklags. Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting. In J. Camp, S. Lewis (eds.) *The Economics of Information Security*, Kluwer Academic Publishers, 2004.

6. G. Aharonian. *Does the Patent Office Respect the Software Community?* IEEE Software, Jul/Aug, 1999.

7. J. R. Allison, M. A. Lemley, K. A. Moore, and R. D. Trunkey. *Valuable Patents.*

George Mason Law & Economics Research Paper No. 03-31; UC Berkeley Public Law Research Paper No. 133. http://ssrn.com/abstract=426020, 2003.

8.   W. Baer, S. Hassell, B. Vollaard. *Electricity Requirements for a Digital Society.* RAND's Publications MR-1617-DOE, 2002.

9.   D. Bainbridge. *Introduction to Computer Law.* Pearson Education, 4th Ed., 2000.

10.   D. Bainbridge. *Software Copyright Law.* Pitman Publishing, 1992.

11.   M. Barrett. *Intellectual Property - Patents, Trademarks & Copyrights.* Emanuel, 1997.

12.   G. Basalla. *The Evolution of Technology.* Cambridge University Press, 1988.

13.   T. A. Bass. *Being Nicholas.* Wired 3.11 - Nov 1995.

14.   W. Bell. *Foundations of Futures Studies.* Vol. 1 and 2, Transaction Publishers, 1997.

15.   Between Concept Scenarios, unpublished report 31.1.2002, Helsinki Institute for Information Technology HIIT, 2002.

16.   E. Blass. *Researching the future: method or madness?* Futures 35, Elsevier, 2003.

17.   M. Castells, *End of Millennium,* Blackwell Publishers, 1999.

18.   M. Castells. Epilogue in P. Himanen. *The Hacker Ethic,* Random House 2001.

19.   M. Castells. *The Rise of the Network Society.* Blackwell, 2nd ed. 2000.

20.   P. Checkland, J. Scholes. *Soft Systems Methodology in Action.* John Wiley & Sons, 1991.

21.   D. Clark. *Face-to-Face with Peer-to-Peer Networking.* Computer Vol. 34, no. 1, January 2001.

22. H. Collins, T. Pinch. *The Golem – What You Should Know about Science.* 2nd ed. Cambridge University Press, 2000.

23. R. G. Cooper, S. J. Edgett, E. J. Kleinschmidt. *Optimizing the stage-gate process: What best-practice companies do-I.* Research Technology Management. Vol. 45, Iss. 5, Sep/Oct 2002.

24. R. Cooter, T. Ulen. *Law and Economics.* Addison-Wesley, 2nd Edition, 1997.

25. K. Coyle. *Rights Expression Languages.* A report for the Library of Congress. 2004.

26. P.A. David. Path dependence, its critics and the quest for 'historical economics'. In P. Garrouste and S. Ioannides (eds.) *Evolution and Path Dependence in Economic Ideas: Past and Present,* 2000.

27. B. Davie, V. Florance, A. Friede, J. Sheehan, J.E. Sisk. *Bringing Health-Care Application to the Internet.* IEEE Internet Computing, May/June 2001.

28. K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, J-C. Burgelman (eds.). *ISTAG Scenarios for Ambient Intelligence in 2010,* Final Report, IPTS-Seville, 2001.

29. S. Dusollier. *Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright.* European Intellectual Property Review, 21:6, 1999.

30. R. Dworkin. *Taking Rights Seriously.* Harvard University Press, 1978.

31. N. Enlund. *Production management for newspapers.* Seybold Newspaper Conference Proceedings, London, 1994.

32. R. Fidler. *Newspapers in 2020: Paper vs. Digital Delivery and Display Media.* Future of Print Media, http://www.futureprint.kent.edu/articles/fidler04.htm, 1999.

33. T. G. Field, Jr. *Intellectual Property: The Practical and Legal Fundamentals.* http://www.fplc.edu/tfield/plfip.htm , 1998

34.   T. G. Field, Jr. *Introduction to Intellectual Property.* Franklin Pierce Law Center, 2000.

35.   J. G. Frynas. *The limits of globalization—legal and political issues in e-commerce.* Management Decision. Vol.40, Iss. 9, 2002.

36.   B. A. Garner (ed.). *Black's Law Dictionary,* 7th ed., West Group, 1999.

37.   P. Goldstein. *Copyright, Patent, Trademark and Related State Doctrines. Cases and Materials on the Law of Intellectual Property.* Fourth Edition. The Foundation Press, Inc., 1997.

38.   S. Guth. *Interoperability of Digital Rights Management Systems via the Exchange of XML-based Rights Expressions.* Vienna University of Economics and Business Administration, 2004.

39.   S. Guth. Rights Expression Languages. In E. Becker et al. (eds.) *Digital Rights Management,* Springer-Verlag, 2003

40.   A. Günther, U. Wuermeling. *Software protection – Germany.* The Computer Law and Security Report, Vol 11 January-February, 1995.

41.   P.-L. Haarmann. *Tekijänoikeus & lähioikeudet.* (In Finnish.) Kauppakaari, 1999.

42.   I. Haikala, J. Märijärvi. *Ohjelmistotuotanto.* (In Finnish.) Suomen ATK-kustannus, 1995.

43.   J. Heikkilä, J. Laine, J. Salo. *Rajat ylittävien etärahapelien sääntely.* (In Finnish.) Defensor Legis N:o 6, 2002.

44.   D. J. Hess. *Science Studies – an advanced introduction.* New York University Press, 1997.

45.   L. Hetemäki. Informaatioteknologian kehitys ja paperituotteet. in R. Seppälä (ed.). *Suomen metsäklusteri tienhaarassa.* (In Finnish) The Finnish Forest Cluster Research Programme Wood Wisdom, 2001.

46. L. Hetemäki, M. Obersteiner. *US Newsprint Demand Forecasts to 2020.* International Institute for Applied Systems Analysis, Interim Report IR-01-070. 2001. http://www.iiasa.ac.at/Research/FOR/, 2001.

47. P. Himanen. *The Hacker Ethic.* Random House 2001.

48. P. B. Hugenholtz. *Code as Code, or The End of Intellectual Property as We Know It.* Maastricht Journal of European and Comparative Law, Volume 6, No. 3, 1999.

49. P. B. Hugenholtz. *The Different Global Copyright Regimes.* Lecture notes at University of Helsinki, 27.9.2001.

50. P. B. Hugenholtz. *The New Database Right: Early Case Law from Europe.* Ninth Annual Conference on International IP Law & Policy, Fordham University School of Law, New York, 2001

51. G. Iacucci, K. Kuutti. *Everyday Life as a Stage in Creating and Performing Scenarios for Wireless Devices.* Personal and Ubiquitous Computing 6:299–306, 2003.

52. R. Jacob, D. Alexander, L. Lane. *A Guidebook to Intellectual Property: Patents, Trade Marks, Copyright and Designs.* Sweet & Maxwell, 2004.

53. H. C. Jehoram. *European Copyright Law - Ever More Horizontal.*

54. S. Jokela, M. Turpeinen. *Ontology Development for Flexible Content.* Proceedings of the HICSS-33, 2000.

55. S. Jokela. *Metadata Enhanced Content Management in Media Companies.* Acta Polytechnica Scandinavica Ma114, The Finnish Academies of Technology, 2001.

56. A. Kankainen. *Thinking Model and Tools for Understanding User Experience Related to Information Appliance Product Concepts.* Doctoral Dissertation, Helsinki University of Technology, 2002.

57. A. Kankainen. *UCPCD: User-Centered Product Concept Design.* Designing for User Experiences, Proceedings of the 2003 conference on Designing for user experiences, 2003.

58. A. Kankainen, T. Kankainen, J. Blom. *Between - Ubiquitous Bubbles Enhancing Human-Human and Human-Computer Interaction.* Final report, 15.5.2003, Helsinki Institute for Information Technology HIIT, 2003.

59. H. Kelsen, M. Knight. *Pure Theory of Law.* Lawbook Exchange, 2001

60. J. Kemppinen. *Oikeus omaan kuvaan.* (In Finnish.) Lakimies, 1997.

61. J. Kemppinen. *Contract-based copyright.* Intellectual property beyond rights, International Conference, IPR University Center, 2004.

62. J. Kemppinen. *Teknologiaoikeuden manifesti.* (In Finnish.) To be published.

63. R. Kilmer. *Peering Beyond the PC. Where P2P Meets the Wireless Web.* IEEE Internet Computing, Vol. 6, No. 3, May – June 2002.

64. M. Koktvedgaard, M. Levin. *Lärobok i immaterial rätt.* (in Swedish) Norstedts Juridik, Sverige, 1992.

65. J. Kontio, O. Pitkänen, R. Sulonen. *Towards Better Software Projects and Contracts: Commitment Specifications in Software Development Projects.* Proceedings of the ICSE'98, IEEE Computer Society, 1998.

66. H. Korth, A. Silberschatz. *Database System Concepts.* 2nd Ed. McGraw-Hill. 1991.

67. J. Laine, I. Ponka. *Kirjallisen muodon täyttäminen sähköisesti.* (In Finnish.) Defensor Legis Nr 6, 2003.

68. A. Lepage. *Overview of Exceptions and Limitations to Copyright in the Digital Environment.* Copyright Bulletin, March 2003.

69.   M. A. Lemley et al. *Software and Internet Law.* Aspen Law & Business, 2000.

70.   L. Lessig. *Open Code and Open Societies.* Keynote address, Free Software — a Model for Society? Tutzing, Germany, June 1, 2000.

71.   L. Lessig. *The Future of Ideas: The Fate of the Commons in a Connected World.* Random House, 2001.

72.   T. Lundmark. *Princess Caroline in Bismark's Shadow: Photographs of Public Figures in German Law.*

73.   T. W. Malone, R. J. Lauerbach, *The Dawn of the E-Lance Economy.* Harvard Business Review, September-October 1998.

74.   M. Mannermaa. Politics + Science = Futures Studies? In J. A. Dator (ed.). *Advancing Futures,* Praeger, 2002.

75.   O. Martikainen. *Complementarities creating substitutes – possible paths from 3G towards 4G and Ad-hoc Networks.* CTIF workshop on Beyond3G/4G, 2005.

76.   R. P. Merges, P. S. Menell, M. A. Lemley. *Intellectual Property in the New Technological Age.* 2nd Ed., Aspen Law & Business, 2000.

77.   R. Merges. *As Many as Six Impossible Patents before Breakfast: Property Rights for Business Concepts and Patent System Reform.* Berkeley Technology Law Journal, 14:2, 1999.

78.   D.G. Messerschmitt, C. Szyperski. *Industrial and Economic Properties of Software: Technology, Processes, and Value.* University of California at Berkeley Computer Science Division Technical Report UCB//CSD-01-1130, Jan. 18, 2001, and Microsoft Corporation Technical Report MSR-TR-2001-11, Jan. 18. 2001.

79.   H. Mintzberg, B. Ahlstrand, J. Lampel. *Strategy Safari: The complete guide through the wilds of strategic management.* Prentice Hall – Financial Times, Pearson Education Limited, 1998.

80. G. Mårtenson, M. Otala, O. A. Wiio. *Tietotekniikka 1990-luvulla.* (In Finnish.) Sitra, B-78, 1985.

81. N.A. Mylonopoulos, G.I. Doukidis. *Mobile business: technological pluralism, social assimilation, and growth.* International Journal of Electronic Commerce. Fall 2003; 8(1), 2003

82. N. A. Mylonopoulos, I. Sideris, K. Fouskas, A. Pateli. *Emerging Market Dynamics in the Mobile Services Industry,* White Paper, the MobiCom Consortium, Research Centre of Athens University of Economics and Business, 2002.

83. J. Mähönen. *Taloustiede lain tulkinnassa.* (In Finnish.) Lakimies 1/2004.

84. N. Negroponte. *Being Digital.* 1995.

85. P. Nikander. *Trustworthiness as an Asset.* Credential-basierte Zugriffskontrolle in offenen, interoperablen IT-Systemen, Dortmund, Germany, 2002.

86. A. M. Odlyzko. *Content is not king.* First Monday 6(2) February 2001.

87. A. Okerson. *Who Owns Digital Works?* Scientific American, 7/96

88. R. Ollila. *Sananvapaus ja yksityisyyden suoja tietoverkoissa.* (In Finnish.) Lakimies 3/2002.

89. S. R. Olson. *Hollywood Planet. Global media and the Competitive Advantage of Narrative Transparency.* Lawrence Erlbaum Associates, 1999.

90. Open Digital Rights Language (ODRL), specification version: 1.1, 2002.

91. K. Paskaleva, S. Curwell, S. Soubra. *Report on Visions and Scenarios.* INTELCITY IST-2001-37373. ITAS, Univ of Salford, VTT, CSTB. 2002.

92. O. Pitkänen, S. Kela. *Sopimukset ja vastuukysymykset dokumenttienhallinnassa.* (In Finnish.) Helsinki University of Technology, Laboratory of Information Processing Science, 2000.

93. O. Pitkänen, M. Välimäki. *Towards A Digital Rights Management Framework.* IeC2000 Proceedings, UMIST, Manchester, UK, 2000.

94. O. Pitkänen, A. Soininen, P. Laaksonen, P. Hurmelinna: *Legal Constraints in Readiness to Exploit Mobile Technologies in B2B.* International Workshop on Wireless Strategy in the Enterprise, Berkeley, CA, 2002.

95. O. Pitkänen, P. Virtanen, M. Välimäki: *Legal Protection of Mobile P2P Databases.* International Conference on Law and Technology (LawTech 2002), Cambridge, MA, USA, 2002.

96. O. Pitkänen, M. Välimäki, J. Kemppinen, M. Mäntylä. *Assessing Legal Challenges on the Mobile Web.* In the Proceedings of M-Business 2002, The First International Conference on Mobile Business Athens, Greece, 2002

97. O. Pitkänen. *Managing Rights in Information Products on the Mobile Internet.* Licentiate's thesis at Helsinki University of Technology, Department of Computer Science and Engineering, HIIT Publications 2002-4, Helsinki Institute for Information Technology HIIT, 2002.

98. O. Pitkänen, M. Mäntylä, M. Välimäki, J. Kemppinen. *Assessing Legal Challenges on the Mobile Internet.* International Journal of Electronic Commerce, Fall 2003, Vol. 8, No. 1, pp. 101-120, 2003.

99. A. Piva, F. Bartolini, M. Barni. *Managing Copyright in Open Networks.* IEEE Internet Computing, Vol. 6, No. 3, May – June 2002.

100. W. K. Pollock. It Pays to "Productize" Customer Services. *The Professional Journal*, AFSM International, August 2000.

101. M. E. Porter. What Is Strategy? *Harvard Business Review*, Novmber-December 1996.

102. R. S. Pressman. *Software Engineering: A Practitioner's Approach.* McGraw-Hill, 2000.

103. J. Pöyhönen. *Oikeustieteen ajanmukaisuus* (in Finnish). Lakimies 3/1997.

104. J. Pöyhönen. *Kohti uutta varallisuusoikeutta* (in Finnish). Lakimies 4-5/1997.

105. J. Pöyhönen. *Uusi varallisuusoikeus* (in Finnish). Talentum, 2003.

106. *Random House Webster's Unabridged Dictionary*, Random House, USA, 1996

107. T. Reti, R. Sarvas. *DiMaS: Distributing Multimedia on Peer-to-Peer File Sharing Networks.* Proceedings of ACM Multimedia 2004 the 12th ACM International Conference on Multimedia, 2004.

108. N. Rosenberg. *Inside The Black Box: Technology and Economics.* Cambridge University Press, 1982.

109. M. Rudanko. *Juridiikka ja liikkeenjohdon strategiat* (in Finnish). Lakimies 4/1999.

110. P. Samuelson. *Good News and Bad News on the Intellectual Property Front.* Communications of the ACM, vol. 42 no. 3, March 1999.

111. P. Samuelson. *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised.* Berkeley Technology Law Journal, 14:2, 1999.

112. P. Samuelson. *Intellectual Property and Contract Law for the Information Age.* California Law Review, vol. 87 no. 1, January 1999.

113. P. Samuelson, R. Davis, M.D. Kapor, J.H. Reichman. *A Manifesto Concerning the Legal Protection of Computer Programs*, Columbia Law Review, Vol. 94:2308, 1994.

114. R. Sarvas. *A Software engineering view to the decisions of European Patent Office concerning computer programs.* Master's thesis at Helsinki University of Technology, 2001.

115. R. Sarvas, M. Viikari, J. Pesonen, H. Nevanlinna. *MobShare: Controlled and Immediate Sharing of Mobile Images.* Proceedings of the 12th annual ACM international conference on Multimedia, 2004.

116. *Scenarios for the Future: Steady Time, Real Time, Zero Time. Our World in 2005.* The Arizona Republic, 2000.

117. E. Schlachter: *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet.* Berkeley Technology Law Journal, Volume 12: Issue 1, Spring 1997.

118. C. Shapiro, H. Varian. *Information Rules: A Strategic Guide to the Network Economy.* Harvard Business School Pr., 1999.

119. M. S. Shapo. *The Law of Products Liability.* 3rd ed. Vol 1- 2. Butterworth Legal Publishers, 1994.

120. M. S. Shapo. *The Law of Products Liability.* 3rd ed. 1998 Cumulative Supplement. Lexis Law Publishing, 1998.

121. A. Soininen. *Tietokoneohjelmien patentointi erityisesti Suomen patenttilain ja Euroopan patenttisopimuksen perusteella..* (In Finnish.) Master's thesis at University of Helsinki Faculty of Law, 2001.

122. A. Soininen (ed.), O. Pitkänen, M. Välimäki, V. Oksanen, T. Reti. *MobileIPR Final Report.* HIIT Publications 2003-3, December 2003.

123. I. Sommerville. *Software Engineering.* Addison-Wesley, 2000.

124. M. Stefik (editor). *Internet Dreams.* The MIT Press, 1997.

125. M. Stefik. *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing.* Berkeley Technology Law Journal, 12:1, 1997.

126. *The Digital Dilemma. Intellectual Property in the Information Age.* Committee on Intellectual Property Rights and the Emerging Information Infrastructure,

Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council. 2000.

127. P. Timmers. *Electronic Commerce: Strategies and Models for Business-to-Business Trading.* John Wiley & Sons, Ltd., 2000.

128. H. Tsoukas. *The Validity of Idiographic Research Explanations.* The Academy Of Management Review, Briarcliff Manor; Oct 1989.

129. K. T. Ulrich, S. D. Eppinger. *Product Design and Development.* Third Edition, McGraw-Hill, 2004

130. U. Varshney, R. J. Vetter, R. Kalakota. *Mobile Commerce: A New Frontier.* Computer Vol. 33, no. 10, October 2000.

131. P. Virtanen. *Database rights in safe European Home: The path to more rigorous protection of information.* Acta Universitatis Lappeenrantaensis 202, Lappeenranta University of Technology, 2005.

132. M. Välimäki. The Challenge of Open Source Licensing – *How Open Source Has Changed the Thinking about Intellectual Property in the Software Industry?* Doctoral thesis, Helsinki University of Technology, 2005.

133. T. Wilhelmsson. *Twelve Essays on Consumer Law and Policy.* Publications of the Department of Private Law 51, University of Helsinki, 1996.

STATUTES AND CONVENTIONS

134. Berne Convention for the Protection of Literary and Artistic Works, WIPO, last amended September 28, 1979.

135. Convention for the Protection of Human Rights and Fundamental Freedoms, the Council of Europe, as it has been amended by Protocol No. 11, 2003.

136. Convention on the Grant on the European Patents (EPC), last amended November 2000.

137. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, 1991.

138. Copyright and Rights in Databases Regulations 1997, Statutory Instrument 1997 No. 3032, the United Kingdom, 1997.

139. Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Directive on products liability), 1985.

140. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

141. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 1996.

142. Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, 1997.

143. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

144. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), 2000.

145. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related

rights in the information society (InfoSoc Directive), 2001.

146. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.

147. General Agreement on Tariffs and Trade, The Uruguay Round Multilateral Trade Negotiations, Agreement on Trade-related aspects of Intellectual Property Rights, including Trade in Counterfeit Goods (GATT TRIPS), 1993.

148. German Law Regulating Copyright to Works of Portraiture and Photography, (Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie, Kunsturheberrechtsgesetz), 1907.

149. Henkilötietolaki (Finnish Data Protection Act), 22.4.1999/523.

150. Laki sosiaali- ja terveydenhuollon asiakasmaksuista (Finnish Act on Charges of Social and Health Care Services), 3.8.1992/734.

151. Perustuslaki (The Constitution of Finland), 11 June, 1999.

152. Rikoslaki (the Penal Code of Finland), 39/1889, last changed 650/2003.

153. Tekijänoikeuslaki (Finnish Copyright Act) 404/1961, last changed 748/1998, 1999.

154. Universal Declaration of Human Rights, United Nations, 1948.

155. U.S. Copyright Act, Title 17, U.S.C.

156. U.S. Patent Act, Title 35 U.S.C.

157. Viestintämarkkinalaki (Finnish Communications Market Act), 23.5.2003/393

158. WIPO Copyright Treaty (WCT), 1996.

PATENTS

159.   Data processing system for hub and spoke financial services configuration, (the so-called *State Street Bank's business method patent*), U.S. patent 5,193,056, issued 1993.

160.   Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers, (the so-called *Priceline.com's reverse auction patent*) U.S. patent 5,794,207, issued 1998.

161.   Method and system for placing a purchase order via a communications network, (the so-called *Amazon.com's 1-click patent*) U.S. patent 5,960,411, issued 1999.

COURT CASES

162.   Feist Publications, Inc. v. Rural Tel. Service Co., 499 U.S. 340, 1991.

163.   Gottschalk v. Benson, 409 U.S. 63, 1972.

164.   In re Alappat, US Court of Appeals, Federal Circuit, 33 F.3d 1526, 1994.

165.   Lexmark International, Inc. v. Static Control Components, Inc., US Court of Appeals, 6th Circuit, October 26, 2004.

166.   Lindqvist, European Court of Justice, C-101/01, 2003.

167.   State Street Bank & Trust v. Signature Financial Services, US Court of Appeals, Federal Circuit, 149 F.3d 1368, 1998.

168.   Surveillance cameras in taxis (in Finnish). The Finnish Data Protection Board, 1/2002.

WEB SITES

169.   America Online, Inc., http://www.corp.aol.com/

170.   Apple iTunes, http://www.apple.com/itunes/

171.   Bluetooth Special Interest Group, http://www.bluetooth.com/

172.   ContentGuard, Inc., http://www.contentguard.com/

173.   Creative Commons, http://www.creativecommons.org/

174.   Digital Object Identifier (DOI), http://www.doi.org/

175.   Electronic Frontier Foundation, http://www.eff.org/

176.   European Judicial Network in civil and commercial matters, *Glossary*, http://europa.eu.int/comm/justice_home/ejn/glossary/glossary_en.htm

177.   D. Howe (ed.) The Free On-line Dictionary of Computing, http://www.foldoc.org/

178.   HyperForum on Long Term Sustainability, California Institute of Technology, http://www.hf.caltech.edu/hf/b3/

179.   I-mode links, http://imodelinks.com/

180.   InfoTrends/CAP Ventures, http://www.infotrends-rgi.com/

181.   Institute for Software Research International, Carnegie Mellon University, http://www.isri.cmu.edu/index.jsp

182.   A. Karila. *Protokollakerrokset*. Tik-110.350 Tietokoneverkot. Lecture notes in Finnish. http://www.tml.hut.fi/Opinnot/Tik-110.350/1999/Kalvot/TKV170299/ Helsinki University of Technology, 17.2.1999.

183.   Napster, Inc., http://www.napster.com/

184.   ODRL - Open Digital Rights Language, http://purl.Internet/ODRL/

185.   Persistent Identifier, http://www.persistent-identifier.de/?lang=en

186.   PhotosToFriends, http://www.photostofriends.com/

187.   The Recording Industry Association of America, Inc. (RIAA), http://www.riaa.org/

188.   J. Schull: *Copying is Good*, http://www.booktechmag.com/cgi-bin/LiveIQue.acgi$rec=3238?btmsic

189.   M. Underwood: *Information Society*, http://www.cultsock.ndirect.co.uk/MUHome/cshtml/index.html

190.   W3C, World Wide Web Consortium, http://www.w3c.org/

191.   Whatis.com, http://whatis.techtarget.com/

192.   Wireless Application Protocol Forum Ltd., http://www.wapforum.org/

193.   XrML - eXtensible rights Markup Language, http://www.xrml.org/

APPENDIX 1: MC2 SCENARIOS

The scenarios have been created in HIIT's Mobile Content Communities (MC2) project. I have not participated in the creation process. Instead, I have analyzed the scenarios from the legal point of view and given comments to the MC2 project team. MC2 project is managed by Dr. MARKO TURPEINEN, and the researchers who have mostly contributed to the scenarios are RISTO SARVAS, TERO LAUKKANEN, ANTTI SALOVAARA, FERNANDO HERRERA, KAI KUIKKANIEMI, KALLE TOISKALLIO, and MIKAEL JOHNSON.

SCENARIO 1: CREATING A STORY FROM MIXED-REALITY GAME SESSION

Jake has come to Helsinki to visit his friend Samuel, who suggests that they go to a hockey game in the evening. Samuel explains to Jake that he has been part of a hockey betting community, named Hobeco, during the whole hockey season. He shows Jake the Hobeco website, which is hosted by Bettaus, a Finnish lottery and betting company. On the website they view match reports and betting analyses written by other members of Hobeco, and some "hot tips" for the evening's game. Samuel proudly tells Jake, that he has been participating actively in the community for the whole hockey season, and therefore has been promoted by the website owners to *moderator*, who can rate the tips and reports made by others.

They create Jake an account on Hobeco and buy tickets for the game from the site. They also place a bet together for the home team: "Let's bet for home victory,

and let's also bet fro the end score to be 3-2 for the home team, we'll trade it during the game if the score is 2-2 or 3-1." Then they take a picture of themselves to be posted on the Hobeco site next to their betting info. "Some people usually follow my bets, which is of course flattering. But now they can see that *you* have made the same bet too, so maybe they'll be scared!", Samuel jokes. "Yeah, blame me if the home team doesn't win and your reputation is gone", Jake laughs. They receive the tickets and game data (player names, numbers, statistics etc.) into their mobile phones, and leave the house for the game.

They take some pictures of the crowd at the arena, and Jake sends few images to his friends back home: "Poor guys, you just have to watch the game from tv...". The game starts, and Jake and Samuel are immersed in the game. They take more pictures, especially of people cheering after each time the home team scores. They also check some player stats from the information package they got from Habeco. In the final period the game is 2-2 and the crowd is full of excitement. "Check out the betting exchange tracker!" Jake shows Samuel his phone's screen, "Someone is selling their bet that the last goal is scored during the final ten minutes. If we combine that bet to our final score bet of 3-2 we could hit paydirt!". They decide to buy the bet and combine it with their owen bet for the final score. "Aargh! I can't bear this excitement. If the home team scores now, we win all three bets!", Jake screams and bangs his fists to his head. "Hahaaa! I caught your anxious face on my camera! Look.", Samuel shows the image to Jake.

The home team scores in the final minute, and the game ends 3-2. Jake and Samuel shout like crazy in their celebration. They go to the bar next to the hockey arena to spend their winnings and watch over and over the replay of the final goal from the Habeco website using their mobile phones.

Next morning they wake up wearing their game jerseys backwards and a minor headache from all the apple juice they drank in the post-game celebrations. "Wake up, Jake. We have to update the website with our photos and comments!" They both upload the images they took to the website, and use the *Game Report Generator* sponsored by the popular "Hockey 2Night" show to put their images into a

multimedia show. The generator automatically interleaves television footage from the game, player statistics, and even commercials between the images Jake and Samuel took before, during, and after the game. "So this is how you make your fancy game videos that you've sent me by email", Jake comments. "Yeah, and I usually post them to the website, too. They give rewards to best shows every month." Jake's mobile phone beeps for a message. "Hey, I got 'minor expert' status from the website because of my correct betting", Jake shouts. "Welcome to the bookie world!" Samuel grins back.

SCENARIO 2: PLAYER-CREATED MOBILE GAMES

Janet, 17, has been playing a multi-player location-aware mobile game with her friends for two months. By now they have played through all the original scenarios and the game has started to feel repetitive and stale. However, Janet and her friends really enjoy the game's basic concept. After one of their game sessions Janet comes up with an idea how the game could be modified and made fresh again. The modified version would be a detective story with a distinct film noir theme. The missions would take place in actual locations around Helsinki where Janet and her friends live.

Janet explains the idea to her friends who like it immediately. None of them are quite sure how to go about executing the idea, though, or if it is even conceivable. While playing the game doesn't require any deeper understanding of the underlying technology, creating a modification is a whole different story. Luckily, one of Janet's friends is aware of the player/modder community at PongForge.net. Pong Forge is the place to be if you are interested in making or modifying mobile games. In addition to tool downloads and tutorials, it has message boards where modders can discuss their ideas, announce releases and ask for help. Each mod project also has its own info page where the authors can post news and pictures. After getting acquainted with the Pong Forge Janet presents her idea to the community. The immediate response is positive: the mod is indeed conceivable and sounds like a great idea - if executed properly. Janet and her friends are glad to hear this and anxious to

get the project going.

Having learned about the different elements of modding, Janet feels that she and her friends can do most work themselves. Janet will personally be responsible for designing the graphics and photographing the mission locations around Helsinki. Photography is her favourite hobby, and for the mod she can flex her creative muscles with stylish black and white pictures. Her friends will help with the mission structure and tagging all the spots in the city. All the project needs is a programmer. From the Pong Forge forums Janet finds a computer science student who happens to be big fan of crime novels. He's interested in doing the coding work, although admits his inexperience with the scripting language in question. Janet is not too worried, as they are all novices anyway. This can be a learning experience for them all.

The project gets underway. Janet and her friends plot the story with a lot of helpful input from the newly recruited coder. The coder also comes up with an idea of how to make the mod easily adaptable to any city. There are some issues about the gameplay structure and balancing that Janet's group have to learn by trial and error. They also don't feel shy about asking for help at the forums, although the responses are not always very helpful nor polite. Janet will not be discouraged by few naysayers, however, as positive support is overwhelming. Once Janet posts the first screenshots on the project page, the sudden buzz surrounding the mod surprises the group completely. Within a week their little learning project is the third most visited project page. Janet starts to feel extra pressure. She has bonded with the community and doesn't want to let anyone down, so she decides that the project has to be carried out super-meticulously. An additional coder and a couple of beta testers are recruited via the message boards.

Finally, after two months of planning, plotting, photographing, tagging, scripting, and testing, the mod is ready to be released. With a ceremonial mood, Janet uploads the mod to Pong Forge and posts an announcement to the message boards. Within minutes the mod is downloaded for the first time. Janet feels exhilarated as the numbers go up. The next morning the mod is already on the top-ten list, and

eventually becomes the most downloaded game in Helsinki for two weeks. The accolades from the community are more than enough reward for Janet's group, but the free cell phones they'll get from a Pong Forge sponsor are definitely a nice bonus.

The pleasure derived from the creative challenge and the community's feedback encourages Janet's crew to start developing a sequel. This time the workload is lightened considerably by the fact that they can recycle many of the elements used in the original. Janet herself is happy, because now the group can concentrate more on the story and its illustration. After two successful sequels, Janet's film noir mod series has established a cult status in the mobile gaming community. Because of the mod's clever design, modders from several cities in Finland have been able to create their own localized versions of the game - with Janet's blessing of course. Janet is also approached by a Swedish modder who would like to adapt the game to Stockholm. Janet has to explain that her product is not really a game but a mod that requires a commercially developed game to work. Currently that game is only available from Finnish operators. After another inquiry from Germany, Janet decides to ask the developer if there are any plans to release the original game abroad. The developer is well aware of Janet's mods and has already been contemplating the idea of branding the film noir mod for commercial release. Together they devise an international release bundle that consists of a film noir themed version of the location-aware mobile game and a toolkit/tutorial for creating localized mods. The mod is also re-branded for domestic release. Janet and her friends will get royalties from the sales, while Janet also becomes a part-time employee of the game development company (until she graduates).

SCENARIO 3: A VISIT TO A MOBILE ONLINE ROLEPLAYING GAME

Jarkko is a player in a mobile multi-player role-playing game. In the game, he is currently managing an important manoeuvre against a competing guild and

therefore he has to check the game status once in a while. Right at the moment Jarkko is waiting for a bus and since there is some time, he checks the game status and decides to notify one player about some details.

The communication in the game is based mainly on push-to-talk technique that allows a quick on-line audio interface between players in the same guild. Right at the moment there is actually some very heated activity going on, and Jarkko tries to grasp an idea of the situation. But the bus enters into a tunnel and the connection cuts off. Jarkko is anxious to know more about what is happening to his guild. He starts repeating "come on, tell me what's going on, ***ing network.." which makes other passengers stare at him. After having asked two times "did you kill them" in a high voice without a reply, he realizes that he cannot lead the team due to the connectivity problems.

The game program notices that Jarkko's guild has lost the connection to its leader, and announces to the rest of the guild that Jarkko cannot manage the situation right now. It selects another player, Matti, from the guild to be the leader of the maneuvre for the time being. This way the guild is saved from an attack. Matti is praised by the others for his bold decisions under the pressure of sudden leadership.

SCENARIO 4: LOCAL SUPER-DISTRIBUTED GAME AND SOCIAL ACCEPTABILITY

There is a wireless local network inside one shopping mall. To tempt new customers to come to shopping mall, the customers can play location-based mobile games with each other using the local network.

John and Mark are playing a game at the mall. The game is based on hiding and finding a secret invisible token. Token can be found by following location based and context based hints, which one can receive in his mobile phone client. All players have their own token, which they can hide and then recapture. When a player controls his own token, he cannot receive information about other tokens. Others can still locate his token, but then player can hide again the token in some place inside the mall. Hiding happens by indicating the location and the more exact position. Other players can find the token by following hints and then guessing the position. The guessing happens by taking a photo from the exact position. The player gets points by finding other tokens. Player looses tokens when someone finds his token or he makes a false guess.

Game is a semi-massive location based game, meaning that anybody can register the game and hide a token, and start finding others. Game runs in weekly modes. There are also special tokens, which are hidden by companies and game author in place. The special tokens include additional price (nice picture, or even a coupon from companies). The weekly winner gets then nominated in a mall bulletin board and intra-advertising system and some special price.

Mary comes to the shopping mall and sees her friends running and wandering around. She doesn't understand what they are doing. She stops them and asks what they are doing. They pause their session and quickly explain what they are playing. They try to encourage Mary to join in. The game is much more fun when there are more gamers involved. And it is especially nice to find a friend's token.

Mary has never been curious about mobile games. However, she has never seen John and Mark so excited about something that they are doing. She feels uncertain if spending her money on the game would be worthwhile. And even if she would like to start playing, there is still problem where can she get the game. It all seems too complicated.

John shows her the game, and Mary wants to try it out. John sends a crippled copy of the game to Mary. Mary tries out the game and really enjoys it. However, after completing, she has hidden her token and found the first special token in fast-

food place in the mall (which gives her two sodas at the price of one) the game stops, and asks her if she wants to purchase the full product. Mary likes the game, so she buys the full version of the game. After Mary has found a 20% discount coupon in the nice girls cloth store she gets so excited that she decides to send a crippled copy of it the game also to her friend Susan over the network.

Mary, John and Mark have such a nice time to play the game that they start to laugh and shout while playing the game. People sitting near at a café wonder what they are doing and some are annoyed. But some get interested and want to also join the game, when they see the advertisement from the mall's intra advertisement channel.

Mark has been the most active player in the game, and he has realized that he has a possibility to win the weekly price. He gets bit too excited and tries to find a token from a female cloth store changing room. In the middle of excitement he gets bit sloppy and accidentally enters a room where an older lady is just changing her clothes. The lady gets extremely annoyed and starts yelling at Mark and the store supervisor comes to see what the problem is. Because of causing problems the store supervisor denies Mark's access to the store. He should be more considerate. The supervisor also reports to the game author about the mishap. Mark gets angry. He was winning and now he cannot get in the store anymore to get the last tokens so he will loose because of that.

SCENARIO 5: SOCIAL PRESSURE AND CONFLICTING MORAL CODES IN VIRTUAL WORLDS

Jogge (14 yrs) has been visiting this place, Habitcity, now about one month. He still does not know how to behave properly. For this reason, it is more comfortable to wander there with his friends. They all have a soldier ranks, and the type of their weapons is indicated in their description text. Some of their big brothers are in the army at the moment, so they know the ranks. About one hour ago, Commander90, boss of their gang, said that now it is Jogge's turn to steal some credits from

someone in this place. If he succeeds, he'll be a full member of this gang. They all have passed this same test.

Jogge is now trying to block the way of some oncoming characters, promising to leave them alone if they will give their password to him. Now a growing amount of non-gangster characters are tightening their circle around Jogge. His pals are not willing to help him at all.

Somebody in the circle says: "OK, we have a newbie here again. Even if we are not in the streets now, and even if there are no written rules in this room, you are not allowed to disturb participants. All the others in the circle shout: "Yes!" Someone else says: "Free moving in this space is essential. This room is for no use if we, you also, as you see my dear friend J, cannot move freely. Peace, man." Another one in the circle continues: "Click the 'villain history' button. There is archived many of this kind of situations. Many of us have tried the same – and learned what really is the purpose of this great site. Jogge! Our dear newbie! As a welcome gift, we will give you the sword of relational trust and personal confidence. As you may already know, it is the strongest weapon that can be used in our combat room - if you happen to feel aggressive some day."

Jogge feels embarrassed. What the hell, are these guys adults or something? Anyway, he wants to try the sword. Wow! His former friends are, of course, in the combat room. His new sword makes him to defeat them easily, all too easily. He feels that the excitement of a battle is fading. A voice in the room asks him: "Jogge, how do you feel with the sword?" Jogge says that it is great, he could actually kill his former friends finitely. Yes, says the voice. Yes you could. That might feel great – but only for a while. So, do as you wish, but I recommend that you think carefully because this community needs also those little bastards. You see, if we would remove them, yes that would be an easy job, stronger villains would come and the borderline between what is thought to be bad and good would move to more severe direction. By the way, have you seen this super combat room, it is available only for those able to really use the sword…"

When Jogge enters that room, the voice asks his mobile phone number and then

gives him a secret number. Jogge is so fascinated about his rising to this new, more adult, and somehow morally upper level that he does not wonder at all so personal questions. By sending an SMS to that number he can pay (2€) the new sword and other stuff needed on this level.

Behind a corner there comes a huge monster and it comes straight-forwardly to Jogge. He doesn't know what to do, when it says: "I can sell you a very good sword and a shield", the monster then says. "I've done them by myself, sort of, you know. They are improved versions of the normal ones... Just give me your mobile phone number..."

Jogge will not give the number, so the monster asks him to follow it and do some services to his gang. Then he would get the stuff...

They pass by a statue and Jogge asks what it is. The Monster says that it is the great founder of our league. Shout with me: "Own sword, fine sword!!"

When they go on their way to the gang premises, it explains: you know, we are against normal weapons. In our opinion, everybody should be able to construct their own swords. The one that you might get is very fashionable at the moment. It has golden stripes, you know. You can trade it very easily, for instance to those poor silver sword gangsters - if you just understand their odd language. Because you need to learn them to use it also, they are so stupid. And ask them how to do the tripplejump, that is what they can do, not so much else.

SCENARIO 6: CHALLENGES IN MANAGING PLAYER PRESENCE AND CONTEXT IN A PERSISTENT MIXED-REALITY GAME

Franck is sleeping in bed when his mobile is ringing. What time is it, he thinks. It is 02.30. Half-sleeping, he picks the phone, and makes accidentally his Tom Clancy book to fall to the floor. Someone gives him orders: Before noon he should kill 5 player characters whose players all work in the same business park as he does. What

the hell?! What are you talking about?

Then he remembers that one month ago he had registered to a mobile conspiracy game called MOGELA, short for Mobile-Geo-$-LARP. The monthly payment was a quite a sum of money, but now he is able to send as much SMSs as he wish. Trying to calm down his enthusiasm, or, paranoid game addiction, as the nosy company doctor had remarked to him, he had promised that this would be the last time for ever, or at least for a while. Now that he is a bit more awake, he sends an SMS to the game server and cancels his registration. He thinks that he very much would like to control his appearance in and off the game to avoid such calls.

"Daaaaddyyyy, is it morning now?" "Just go on sleeping Mikke, phone just rang, and don't wake up your little sister."

In the morning Franck is driving from kindergarten to his job, thinking relaxed that fortunately the kindergarten doesn't know his current salary. If it would, then he would need to pay full payments for the day care. Then his smart phone in the dashboard rack rings announcing arrival of a new email: longitude and latitude coordinates and an announcement that in the location there would be a hidden plastic "shell" that would contain the instructions of his next tasks and the role in the game. While routinely inserting the coordinates into his smart phone's GPS function, he is still wrestling with the pros and cons of continuing this hobby - and wondering also why he got this message after quitting, anyway. Did the server somehow lose his cancellation? If things like this happen, he realizes, maybe also his current income is no secret to the kindergarten. Actually, that would explain why the kindergarten staff looked at him little oddly, he worries paranoidically.

He hears an email beeping again.

The honoured moderator of the Scandinavian section of MOGELA community herself regrets the inconvenient call Franck got last night. He hopes that Franck is still willing to continue his membership in MOGELA and keep his membership profile active in the location-based mobile connectivity service, to be able to send and receive messages of other road-users belonging to MOGELA. All his 5 closest

friends (Jack, Nick, Dick, Steve and Bor) are seriously worried of his intention to quit playing the game. Actually, 158 members of the community, all of them being a friend, or a friend of a friend of Franck, kindly ask him to stay. Otherwise this new community might collapse, they say.

Franck thinks that this is a routine persuasion tactic. However, it feels good to be needed.

Furthermore, the moderator continues, 68 persons ("Franck, they are all your friends, or, friends of your friends") in this community, driving now in the same city, are saying to him that "Why not to use merely the jam and police alert function, if the conspiracy game is too frustrating. 20 avoided traffic jams or 5 (obvious) speeding tickets makes you the star of the month! Then you can organize our collective AVEVs, avoiding events. In conspiracy you feel always as being on the side track, sort of marginal, you know. But we the FOCA people are all with you. Feel the Force - Of Collective Avoiding. Support this sub-community and buy a FOCA sticker to your bumper. Only press the green button of your mobile, and pay your phone bill."

This new and obviously "semi-legal" faction of this conspiracy game is a surprise to Franck. Can he trust fully that this kind of internal help in a subcommunity would really work? Or is it just a trick? Are they trying to get him in problems with the police?

His smart phone beeps announcing that he is approaching the announced location, and he pulls over to the gas station (Shell, yeah, of course, he thinks sarcastically) and begins to look at the encrypted hints, to be able to find the hidden box. He decrypts the hint message using the smart phone, and the message says: You should buy today's "Evening News" and a Coke. When you have found these "two of the four required elements" and thus got closer to "the real thing", you should reward yourself with the Coke. Enthusiastically Franck walks towards the gas station's counter.

Franck promises to himself that TOMORROW he will REALLY quit the game.

SCENARIO 7: CONTEXT SENSITIVE ADVERT GAMING

SCENARIO DESCRIPTION

Mary and her sister Marie have gone to see the latest Hollywood blockbuster after spending all day together at school. They arrive to pick-up their reserved tickets. After they get their ticket, it hits them: they have a whole hour to wait before the movie starts. They look for something to do.

Hanging out in the theater they see posters for a new mango soda all over the place. The posters encourage them to download the freely available mango soda mini game, all those who get more than 2000 points get a free soda, and 40000 points a free soda popcorn combo. The only catch is… the game can only be played at the theater and players can only win one price/day. They decide to try it out and download the game to their phones. They have fun playing and avidly compare their scores as they go. Time flies and suddenly they are already seating in the cinema room. As the room darkens and the usual pre-movie commercial start. They see a big advertisement on the screen for the new soda, and it shows the names of the top 10 players of the day. Mary and Marie get impressed as they see their school friend John's screen name flashing on the big screen. John is the top scorer of all times.

When they arrive home and turn on the television. John's name is on TV right next to the Super Mango Cola logo on a commercial. John has won a year supply of movie tickets.

SCENARIO 8: COMPANY-COMMUNITY RELATIONS IN CONTROLLING USER-CREATED CONTENT

The first five years of the global online game-play community could easily be described as a brief establishment phase followed by rapid growth. The gaming platform had some unique characteristics, but the key to the initial success was the well defined policies and code of conduct that matched the target audience. The rapid growth was managed nicely by the company that created the game. Despite the increasing diversity, the lead developers managed to scale the game well in the different national cultures, maintaining the feeling of the community.

Actually the gaming platform itself was not a game, but an environment where the players themselves could modify their avatars and the in-game environment, as well as create their own games by defining their own winning conditions. Many preferred not to compete at all, they just explored the game and used it to socialize with their friends.

Now, halfway through the second five years of the global community, the leading developers in the company were a little uneasy. The popularity of the game in one country had rapidly decreased, but they didn't understand why. None of the polls and interviews that the local marketing group had conducted had resulted in any reliable explanation of the decline. Despite the efforts to identify new leaders and maintain trust and openness, some player groups continued to ignore the rules.

"Damn it!" said one of the founding mothers of the game, "who's game is this anyway?" She was tired of the new mods that threatened the public good, and afraid that they would spread to the other national game-play communities. They had hoped that they could gradually decrease the influence of the staff, and let the community members take more control, as the experienced community builder Amy Jo Kim already in the year 2000 had predicted would be possible in mature communities.

This malicious and ingenious mod had taken advantage of a hole in the licensing policy of the game. The company had wanted to encourage modding, letting the

people freely create and keep copyright of mods that only change the audiovisual elements of the game. The developers had assumed that audiovisual mods couldn't influence the game mechanics, but that was clearly not true in this case. The problem was that taking care of this hole in the licensing policy would change the game world and make some of the most successful and popular mods impossible. The game developers had conducted several global and national polls on this issue, to investigate how many would quit playing the game if the modification possibilities were reduced as drastically as the IPR-professionals suggested.

The unexplainable fact was that this issue seemed to create a sharp line within the well-known player groups. Heavy users, regulars, lurkers, dominators, weavers, gurus, defenders, needlers, newbies - all seemed to be on both sides of the issue. No variable - gender, age in RL, age in community, modding skills, level of commitment, etc. - seemed to explain it, and the game developers didn't know how to decide on the issue since there were no clear groups to follow. The issue seemed to have raised a previously unknown dimension to the community, and the consequences of either way were deemed unpredictable.

In this frustrating situation that threatened to tear the company apart with people taking sides on the issue, it seemed like a lose-lose situation. The game developers wanted to collaboratively brainstorm ideas before the decision and had gathered an emergency community development council to take place online in one of the restricted areas of the game environment. Representatives of each player group from each national community and the game leaders were having a brain-jamming session.

Suddenly, an avatar from the North raised his virtual hand to get the floor. "I know a friend, who knows a group that has some very elaborate community models - including community life cycle, modding effects and the tension between corporate and participative cultures - shouldn't we consult them?" he asked. "Yeah", said another avatar that was dressed like an elderly woman: "Let's call The Researchers!".

Epilogue. One year after The Researchers' suggestion that the communities should be able to create and implement their own sanctions when members continue

to ignore the rules, the situation was much less dramatic. Many sanctions that stopped some of the worst issues had been implemented on a very local level, before the issues could spread to a larger audience. But, as always, the sanction-policy wasn't perfect either. There had been some smaller events when the sanction system itself had taken some abuse. Still, the developers considered this a minor issue compared to the crisis before. In fact, the developers had been playing the function of the government, and as they wanted to let go of the control, they had forgot that they needed to create some institution dealing with justice.

APPENDIX 2: ISTAG SCENARIOS

The summaries of ISTAG scenarios are cited below. They have been created by the IST Advisory Group (ISTAG). The scenarios are discussed in more detail in K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, J-C. Burgelman (eds.): *Scenarios for Ambient Intelligence in 2010*, Final Report, IPTS-Seville, 2001.

SCENARIO 1: 'MARIA' – ROAD WARRIOR

After a tiring long haul flight Maria passes through the arrivals hall of an airport in a Far Eastern country. She is travelling light, hand baggage only. When she comes to this particular country she knows that she can travel much lighter than less than a decade ago, when she had to carry a collection of different so-called personal computing devices (laptop PC, mobile phone, electronic organisers and sometimes beamers and printers). Her computing system for this trip is reduced to one highly personalised communications device, her 'P–Com' that she wears on her wrist. A particular feature of this trip is that the country that Maria is visiting has since the previous year embarked on an ambitious ambient intelligence infrastructure programme. Thus her visa for the trip was self-arranged and she is able to stroll through immigration without stopping because her P-Comm is dealing with the ID checks as she walks.

A rented car has been reserved for her and is waiting in an earmarked bay. The car opens as she approaches. It starts at the press of a button: she doesn't need a key. She still has to drive the car but she is supported in her journey downtown to the conference centre-hotel by the traffic guidance system that had been launched by the

city government as part of the 'AmI-Nation' initiative two years earlier. Downtown traffic has been a legendary nightmare in this city for many years, and draconian steps were taken to limit access to the city centre. But Maria has priority access rights into the central cordon because she has a reservation in the car park of the hotel.

Central access however comes at a premium price, in Maria's case it is embedded in a deal negotiated between her personal agent and the transaction agents of the car-rental and hotel chains. Her firm operates centralised billing for these expenses and uses its purchasing power to gain access at attractive rates. Such preferential treatment for affluent foreigners was highly contentious at the time of the introduction of the route pricing system and the government was forced to hypothecate funds from the tolling system to the public transport infrastructure in return.

In the car Maria's teenage daughter comes through on the audio system. Amanda has detected from 'En Casa' system at home that her mother is in a place that supports direct voice contact.

However, even with all the route guidance support Maria wants to concentrate on her driving and says that she will call back from the hotel.

Maria is directed to a parking slot in the underground garage of the newly constructed building of the Smar-tel Chain. She is met in the garage by the porter – the first contact with a real human in our story so far! He helps her with her luggage to her room. Her room adopts her 'personality' as she enters. The room temperature, default lighting and a range of video and music choices are displayed on the video wall. She needs to make some changes to her presentation – a sales pitch that will be used as the basis for a negotiation later in the day. Using voice commands she adjusts the light levels and commands a bath. Then she calls up her daughter on the video wall, while talking she uses a traditional remote control system to browse through a set of webcast local news bulletins from back home that her daughter tells her about. They watch them together.

Later on she 'localises' her presentation with the help of an agent that is

specialised in advising on local preferences (colour schemes, the use of language). She stores the presentation on the secure server at headquarters back in Europe. In the hotel's seminar room where the sales pitch is take place, she will be able to call down an encrypted version of the presentation and give it a post presentation decrypt life of 1.5 minutes. She goes downstairs to make her presentation… this for her is a high stress event. Not only is she performing alone for the first time, the clients concerned are well known to be tough players. Still, she doesn't actually have to close the deal this time. As she enters the meeting she raises communications access thresholds to block out anything but red-level 'emergency' messages. The meeting is rough, but she feels it was a success. Coming out of the meeting she lowers the communication barriers again and picks up a number of amber level communications including one from her cardio-monitor warning her to take some rest now. The day has been long and stressing. She needs to chill out with a little meditation and medication. For Maria the meditation is a concert on the video wall and the medication….a large gin and tonic from her room's minibar.

SCENARIO 2: 'DIMITRIOS' AND THE DIGITAL ME' (D-ME)

It is four o'clock in the afternoon. Dimitrios, a 32 year-old employee of a major food-multinational, is taking a coffee at his office's cafeteria, together with his boss and some colleagues. He doesn't want to be excessively bothered during this pause. Nevertheless, all the time he is receiving and dealing with incoming calls and mails.

He is proud of 'being in communication with mankind': as are many of his friends and some colleagues. Dimitrios is wearing, embedded in his clothes (or in his own body), a voice activated 'gateway' or digital avatar of himself, familiarly known as 'D-Me' or 'Digital Me'. A D-Me is both a learning device, learning about Dimitrios from his interactions with his environment, and an acting device offering communication, processing and decision-making functionality. Dimitrios has partly 'programmed' it himself, at a very initial stage. At the time, he thought he would 'upgrade' this initial data periodically. But he didn't. He feels quite confident with his

D-Me and relies upon its 'intelligent' reactions.

At 4:10 p.m., following many other calls of secondary importance – answered formally but smoothly in corresponding languages by Dimitrios' D-Me with a nice reproduction of Dimitrios' voice and typical accent, a call from his wife is further analysed by his D-Me. In a first attempt, Dimitrios' 'avatar-like' voice runs a brief conversation with his wife, with the intention of negotiating a delay while explaining his current environment. Simultaneously, Dimitrios' D-Me has caught a message from an older person's D-Me, located in the nearby metro station. This senior has left his home without his medicine and would feel at ease knowing where and how to access similar drugs in an easy way. He has addressed his query in natural speech to his D-Me. Dimitrios happens to suffer from similar heart problems and uses the same drugs. Dimitrios' D-Me processes the available data as to offer information to the senior. It 'decides' neither to reveal Dimitrios' identity (privacy level), nor to offer Dimitrios' direct help (lack of availability), but to list the closest drug shops, the alternative drugs, offer a potential contact with the self-help group. This information is shared with the senior's D-Me, not with the senior himself as to avoid useless information overload.

Meanwhile, his wife's call is now interpreted by his D-Me as sufficiently pressing to mobilize Dimitrios. It 'rings' him using a pre-arranged call tone. Dimitrios takes up the call with one of the available Displayphones of the cafeteria. Since the growing penetration of D-Me, few people still bother to run around with mobile terminals: these functions are sufficiently available in most public and private spaces and your D-Me can always point at the closest…functioning one! The 'emergency' is about their child's homework. While doing his homework their 9 year-old son is meant to offer some insights on everyday life in Egypt. In a brief 3-way telephone conference, Dimitrios offers to pass over the query to the D-Me to search for an available direct contact with a child in Egypt. Ten minutes later, his son is videoconferencing at home with a girl of his own age, and recording this real-time translated conversation as part of his homework. All communicating facilities have been managed by Dimitrios' D-Me, even while it is still registering new data and managing other queries. The Egyptian correspondent is the daughter of a local

businessman, well off and quite keen on technologies. Some luck (and income…) had to participate in what might become a longer lasting new relation.

SCENARIO 3: CARMEN - TRAFFIC, SUSTAINABILITY & COMMERCE

It is a normal weekday morning. Carmen wakes and plans her travel for the day. She wants to leave for work in half an hour and asks AmI, by means of a voice command, to find a vehicle to share with somebody on her route to work. AmI starts searching the trip database and, after checking the willingness of the driver, finds someone that will pass by in 40 minutes. The invehicle biosensor has recognised that this driver is a non-smoker – one of Carmen requirements for trip sharing. From that moment on, Carmen and her driver are in permanent contact if wanted (e.g. to allow the driver to alert Carmen if he/she will be late). Both wear their personal area networks (PAN) allowing seamless and intuitive contacts.

While taking her breakfast coffee Carmen lists her shopping since she will have guests for dinner tonight. She would like also to cook a cake and the e-fridge flashes the recipe. It highlights the ingredients that are missing milk and eggs. She completes the shopping on the e-fridge screen and asks for it to be delivered to the closest distribution point in her neighbourhood. This can be a shop, the postal office or a franchised nodal point for the neighbourhood where Carmen lives. All goods are smart tagged, so that Carmen can check the progress of her virtual shopping expedition, from any enabled device at home, the office or from a kiosk in the street. She can be informed during the day on her shopping, agree with what has been found, ask for alternatives, and find out where they are and when they will be delivered.

Forty minutes later Carmen goes downstairs onto the street, as her driver arrives. When Carmen gets into the car, the VAN system (Vehicle Area Network) registers her and by doing that she sanctions the payment systems to start counting. A micro-payment system will automatically transfer the amount into the e-purse of

the driver when she gets out of the car.

In the car, the dynamic route guidance system warns the driver of long traffic jams up ahead due to an accident. The system dynamically calculates alternatives together with trip times. One suggestion is to leave the car at a nearby 'park and ride' metro stop. Carmen and her driver park the car and continue the journey by metro. On leaving the car, Carmen's payment is deducted according to duration and distance.

Out of the metro station and whilst walking a few minutes to her job, Carmen is alerted by her PAN that a Chardonnay wine that she has previously identified as a preferred choice is on promotion. She adds it to her shopping order and also sets up her homeward journey with her wearable. Carmen arrives at her job on time.

On the way home the shared car system senses a bike on a dedicated lane approaching an intersection on their route. The driver is alerted and the system anyway gives preference to bikes, so a potential accident is avoided. A persistent high-pressure belt above the city for the last ten days has given fine weather but rising atmospheric pollutants. It is rush hour and the traffic density has caused pollution levels to rise above a control threshold. The city-wide engine control systems automatically lower the maximum speeds (for all motorised vehicles) and when the car enters a specific urban ring toll will be deducted via the Automatic Debiting System (ADS).

Carmen arrives at the local distribution node (actually her neighbourhood corner shop) where she picks up her goods. The shop has already closed but the goods await Carmen in a smart delivery box. By getting them out, the system registers payment, and deletes the items from her shopping list. The list is complete. At home, her smart fridge screen will be blank.

Coming home, AmI welcomes Carmen and suggests to telework the next day: a big demonstration is announced downtown.

SCENARIO 4: ANNETTE AND SOLOMON IN THE AMBIENT FOR SOCIAL LEARNING

It is the plenary meeting of an environmental studies group in a local 'Ambient for Social Learning'. The group ranges from 10 to 75 years old. They share a common desire to understand the environment and environmental management. It is led by a mentor whose role it is to guide and facilitate the group's operation, but who is not necessarily very knowledgeable about environmental management. The plenary takes place in a room looking much like a hotel foyer with comfortable furniture pleasantly arranged. The meeting is open from 7.00-23.00 hours. Most participants are there for 4-6 hours. A large group arrives around 9.30 a.m. Some are scheduled to work together in real time and space and thus were requested to be present together (the ambient accesses their agendas to do the scheduling).

A member is arriving: as she enters the room and finds herself a place to work, she hears a familiar voice asking "Hello Annette, I got the assignment you did last night from home: are you satisfied with the results?" Annette answers that she was happy with her strategy for managing forests provided that she had got the climatic model right: she was less sure of this. Annette is an active and advanced student so the ambient says it might be useful if Annette spends some time today trying to pin down the problem with the model using enhanced interactive simulation and projection facilities. It then asks if Annette would give a brief presentation to the group. The ambient goes briefly through its understanding of Annette's availability and preferences for the day's work. Finally, Annette agrees on her work programme for the day.

One particularly long conversation takes place with Solomon who has just moved to the area and joined the group. The ambient establishes Solomon's identity; asks Solomon for the name of an ambient that 'knows' Solomon; gets permission from Solomon to acquire information about Solomon's background and experience in Environmental Studies. The ambient then suggests Solomon to join the meeting and to introduce himself to the group.

In these private conversations the mental states of the group are synchronised with the ambient, individual and collective work plans are agreed and in most cases checked with the mentor through the ambient. In some cases the assistance of the mentor is requested. A scheduled plenary meeting begins with those who are present. Solomon introduces himself. Annette gives a 3-D presentation of her assignment. A group member asks questions about one of Annette's decisions and alternative visualisations are projected. During the presentation the mentor is feeding observations and questions to the ambient, together with William, an expert who was asked to join the meeting. William, although several thousand miles away, joins to make a comment and answer some questions. The session ends with a discussion of how Annette's work contributes to that of the others and the proposal of schedules for the remainder of the day. The ambient suggests a schedule involving both shared and individual sessions.

During the day individuals and sub-groups locate in appropriate spaces in the ambient to pursue appropriate learning experiences at a pace that suits them. The ambient negotiates its degree of participation in these experiences with the aid of the mentor. During the day the mentor and ambient converse frequently, establishing where the mentor might most usefully spend his time, and in some cases altering the schedule. The ambient and the mentor will spend some time negotiating shared experiences with other ambients – for example mounting a single musical concert with players from two or more distant sites. They will also deal with requests for references / profiles of individuals. Time spent in the ambient ends by negotiating a homework assignment with each individual, but only after they have been informed about what the ambient expects to happen for the rest of the day and making appointments for next day or next time.