Legal Research Topics within Services Sciences

Dr. Olli Pitkänen
Helsinki Institute for Information Technology HIIT
e-mail: olli.pitkanen@hiit.fi

Abstract

The paper presents a study to define some of the most important legal topics that need to be included in the Services Sciences' research agenda.

To analyze what sort of legal challenges the forthcoming services will have, an example of advanced service framework, MobiLife Service Framework, is presented. The framework highlights especially challenges in privacy and data protection and intellectual property rights.

The analysis is complemented with a discussion on some other scenarios and examples that bring out legal issues. Based on the analysis, the paper concludes the most important legal topics that should be studied further in relation to services sciences in the fields of privacy and data protection, intellectual property rights, and contracts.

1 Introduction

Services sciences, Management and Engineering is an emerging discipline bringing together ongoing work in computer science, operations research, industrial engineering, business strategy, management sciences, social and cognitive sciences, and legal sciences to develop the skills required in a services-led economy.[5]

This paper presents a study that defines some of the most important legal topics be included in the Services Sciences' research agenda.

To analyze what sort of legal challenges the forthcoming services will have, an advanced service framework is presented and its legal issues are discussed.

2 MobiLife Service Framework

MobiLife is an Integrated Project (IST-511607, http://www.ist-mobilife.org/) in European Union's 6th Framework Programme. It is to bring advances in mobile applications and services within the reach of users in their everyday life by innovating and deploying new applications and services based on the evolving capabilities of 3G systems and beyond.

MobiLife has introduced a mobile service framework that identifies the essential functional blocks for the implementation of the new mobile services and applications, and relations between them. According to MobiLife document D43b, the Basic Reference Model is a framework for understanding significant relationships among the components of the MobiLife service provisioning architecture, and for the development of consistent specifications supporting this environment. It fulfils the following set of requirements.[11]

The mobile services framework:

- shall support legacy as well as emerging applications,
- shall support the usage of contextual information,
- shall support context management,
- shall support service personalisation,
- shall support both managed services and non-managed ("ad hoc") services,
- shall support emerging value nets,

- shall support seamless service access via multiple access technologies,
- shall consider privacy and trust issues and support relevant solutions, and
- shall provide service and component lifecycle support.

Contextual information includes low-level context data such as location, time, temperature, noise, as well as higher-level context data such as user situation ('in a meeting', 'with friends'). Context data gathered from various sources should influence which services are provided to the user as well as how the services are defined. A simple example of using context information is to determine the location using data provided by the terminal. Additionally, network functionalities can be used in determining the location. Location may have influence on the content of the service, e.g., a service shows the weather of the actual location. [11]

Context data management is an essential part of context aware systems. Different types of context data originate from various distributed sources. This data must be gathered and made available to those components that need them. Access for the context reasoning mechanism to such data should be provided and the results made available to others. For learning process, a history of all past context information should also be stored. Suitable mechanism to store context data along with their history information efficiently is essential. [11]

Personalisation includes the ability of the framework to acquire and manage personal information about the user, including user preferences, and the ability to use this information to adapt an application's behaviour to specific user needs. End users may affect device characteristics by configuring its parameters. Additionally, users may have global preferences affecting all services and specific service settings, e.g., their favourite language. [11]

Managed services and non-managed ("ad hoc") services. The framework supports services that are controlled and maintained by a service provider, e.g., through a service portal, as well as services that are provided in an ad hoc manner directly between users without the control of a third party, e.g., pure peer-to-peer services. [11]

Support for *emerging value nets* implies that the framework is not restricted to current provider – consumer value chains, but shall be flexible regarding new ways of service provisioning such as new ways of incorporating 3rd party service providers. [11]

The framework is to support relevant solutions for *privacy and trust* issues, because privacy and trust are among the most important features to increase user acceptance of services and to achieve customer acceptance. [11]

The six essential building blocks of the MobiLife Basic Reference Model are

- personalisation,
- adaptation,
- context awareness,
- privacy and trust,
- service management, and
- service usage. [11]

The terminal devices and additional sensors provide raw data that are sent to the *context-awareness* function. The raw data makes up context information, such as location data, and are utilised together with device capabilities. The context awareness function is related to the service usage function, the personalisation function, the user interface adaptation function, and also to the services and applications. All these functions need context data to fulfil their functionality, and to provide further context data to the context awareness function. The context awareness function takes care of raw, interpreted and aggregated context data related to individual users and to groups of users. [11]

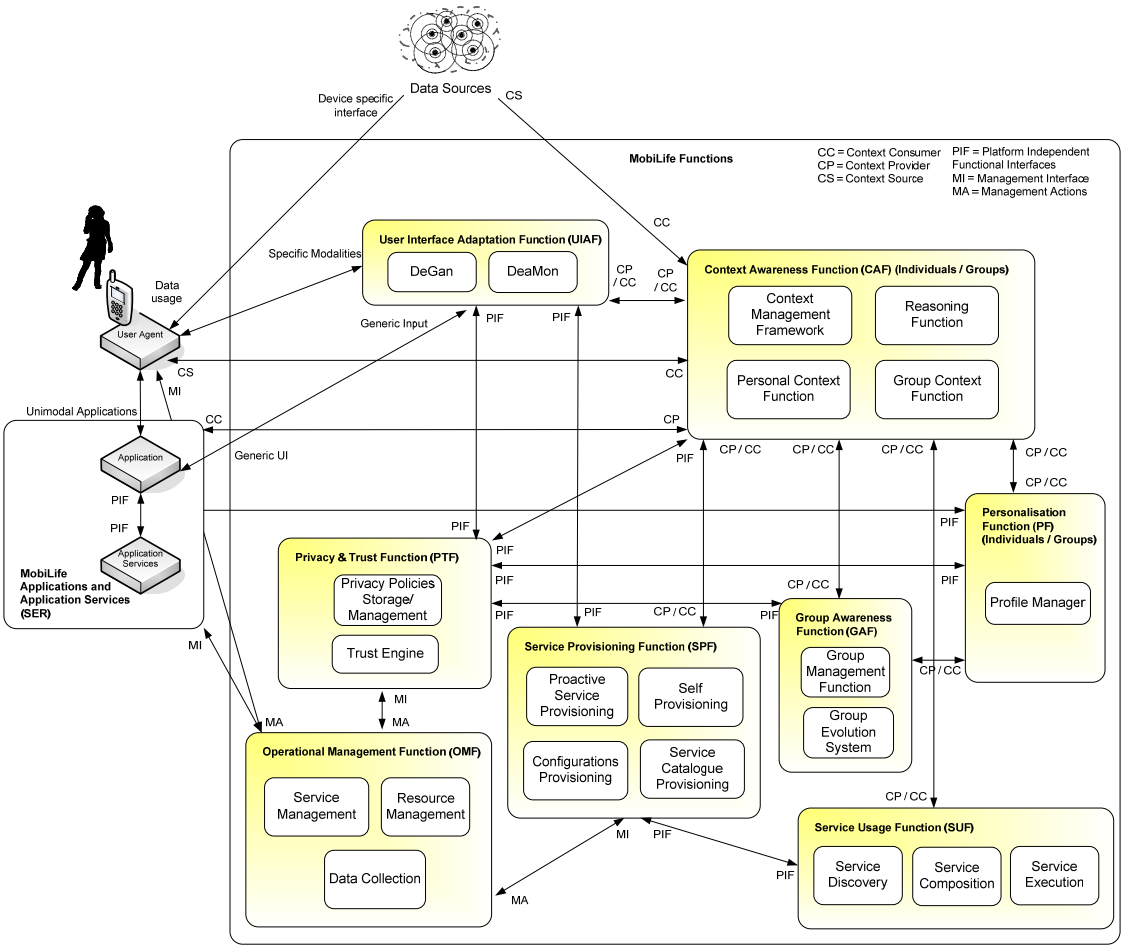

Figure 1. MobiLife Reference Model. [11]

The *personalisation* function provides profiles and preferences of users and groups to the context-awareness function, and support profile learning mechanisms. To support user feedback for profile learning, it is directly related to the services and applications. [11]

The *privacy and trust* support is related to the context awareness function and the personalisation function to provide them with functions and information concerning privacy and trust. [11]

The *service usage* function operates on behalf of the context awareness function. It provides information about the services in the system and supports various forms of service triggering. [11]

The user interface *adaptation* function takes the available relevant context information to facilitate user interface adaptability for services and applications. The function adapts both users' input modalities as well as services' output. User input adaptation function is also related to other adaptations, such as service quality adaptation. [11]

The *service management* function supports the lifecycle of services. To perform this, it needs access to information about services stored in the service usage function. This fact is not shown in the current functional model, but has to be reflected when modelling the physical distribution of the components, i.e. in the system model. [11]

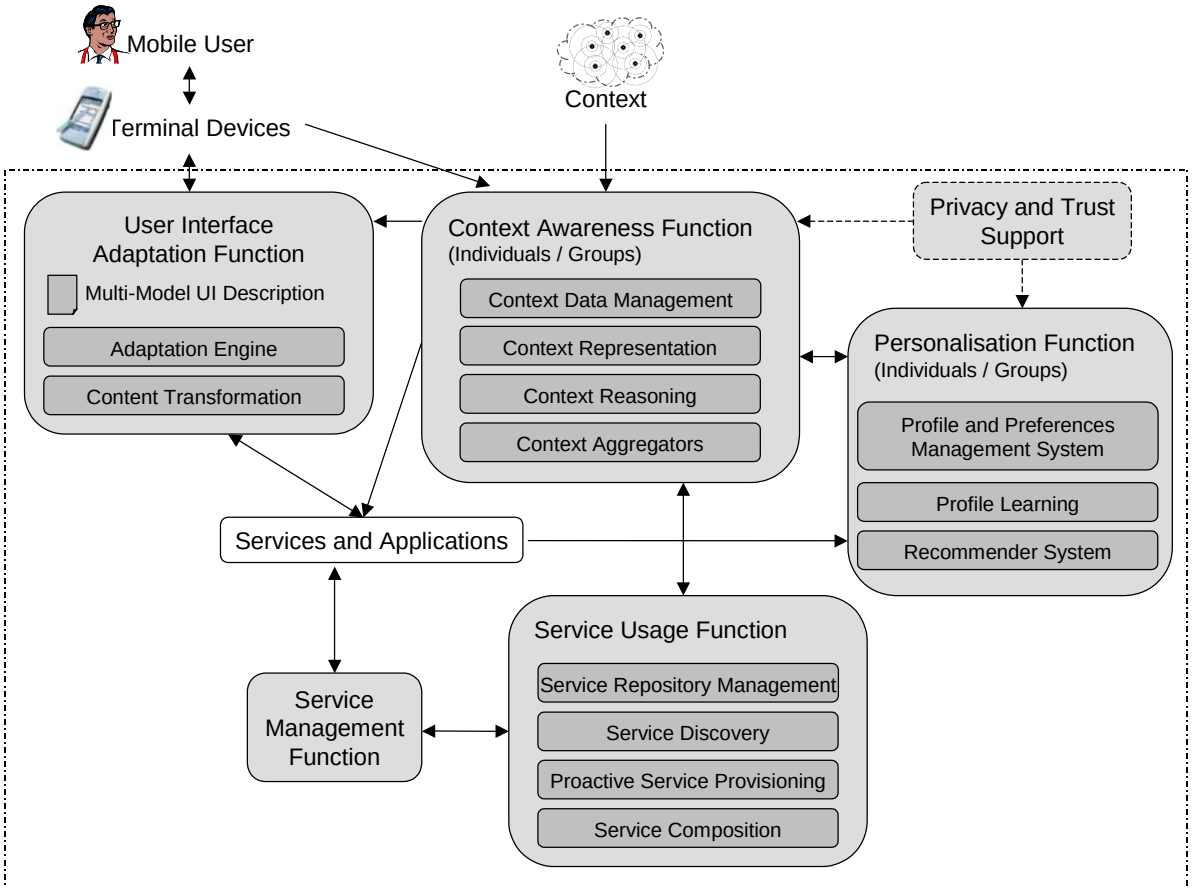

Figure 2. Functional view, MobiLife reference model [11]

3 Legal Issues Arisen by the Framework

According to RÄISÄNEN et al: "If privacy is not guaranteed for a user, there will not be sufficient trust towards the system. If users do not trust the system, they will not use it." [11] This represents well the technology-oriented viewpoint that is characteristic to MobiLife scenarios, service framework, and applications. It implies that the technology alone is responsible for privacy protection and the end-user's privacy expectations are targeting only the technology. While it provides a reasonable starting point for the technology development in MobiLife, in legal analysis, other aspects need to be considered also.

First, it is possible that, in addition to the technology, other factors also support privacy; especially, the legal and moral systems in the society.

Second, it is plausible that the technology fails, which makes it more important to have alternative means to protect privacy.

Third, even today people are using technologies that they don't fully trust. For example, most people seem to believe that Microsoft products are not trustworthy, but still use them. According to Forrester Research survey, three-fourths of software security experts at major companies do not believe Microsoft's products are secure. While 77 percent of respondents said security was a top concern when using Windows, 89 percent still use the software for sensitive applications.[10] Therefore, trustworthy is hardly the primary criteria for end-users to choose technologies.

According to ACQUISTI & GROSSKLAGS, surveys and experiments have uncovered a dichotomy between stated attitudes and actual behaviour of individuals facing decisions affecting their privacy and their personal information security. Surveys report that most individuals are concerned about the security of their personal information and are willing to act to protect it. Experiments reveal that very few individuals actually take any action to protect their personal information, even when doing so involves limited costs. The factors that that could influence the individual are

1. Limited information, and, in particular, limited information about benefits and costs.
2. Bounded rationality.
3. Psychological distortions.
4. Ideology and personal attitudes.
5. Market behaviour.[1]

It seems that technologies as such have little possibilities to directly affect individuals' behaviour with respect to personal information safety, but obviously they have a most important indirect effect. And, of course, even if it is unlikely that the technologies will ever become perfect and flawless, it is still important to try to develop as good technologies as ever possible in projects like MobiLife. Yet, it still pays to study also other means, like regulative and legal aspects, to protect privacy.

According to GARY T. MARX, Professor Emeritus of Sociology, M.I.T., many business and government leaders have an unquestioned, optimistic, over-simplified faith in science and technology as solutions to social issues. Such leaders argue for unleashing technology and maximising economic and security values above everything else. Numerous "techno-fallacies" are commonly heard in such advocacy. The fallacies may be empirical, logical and/or at the level of values. Along with positive policies, laws and technical developments, there is a need to continually interrogate culture and to critically question the assumptions that accompany the creation and implementation of new technologies and related information environments.[2]

Obviously, the technology has also potential to regulate by enabling or disabling behaviour, in comparison with the law that regulates mainly by imposing sanctions. Also, the law has significant limitations. Many undesirable phenomena are out of the reach of the legal system: the law cannot effectively control issues that are hidden or that are not considered to be within the subject matter of the legal system (but e.g. ethical). The technology does not have the same limitations: it is often possible to technologically control issues that are out of the range of the law. Then again, the law can also regulate by influencing the development of the technology. Therefore, it is necessary to consider these approaches simultaneously: should the law, the technology, or the socio-economic environment and conditions be changed? [4][7]

As mentioned above, the six essential building blocks of the MobiLife Basic Reference Model are personalisation, adaptation, context awareness,

privacy and trust, service management, and service usage. Each of them includes some legal concerns.

The *personalisation* function provides other functions with profiles and preferences of users and groups. In other words, it processes personal data – unless the profiles and preferences are anonymized in a way that makes it impossible to relate it to an identifiable person. Therefore, especially in Europe, data protection law is often applicable. The collector of data should be able to articulate the specified, explicit and legitimate purpose for which the data is collected. The data should not be further processed in an incompatible way with that purpose and no inadequate, irrelevant or excessive data in relation to the purpose must be processed. The processing of incorrect or incomplete information can cause significant damage to the data subject. It must be taken care of that any major decisions are not made based on wrong or partial information. In the European Union, the Data Protection Directive restricts completely automated individual decisions which produce legal effects concerning the data subject or significantly affects him and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. In the USA, data protection rules are more relaxed, but should not be ignored either. Thus, privacy and data protection law may significantly impact the personalization function.

The *context awareness* function has additional data protection issues compared to personalization. First, the automatic fetching of context information, i.e. information about the circumstances of a private person, can make it more difficult to clearly define what information is processed and to inform the person on the processing of that data. Second, the processing of context information involves not only the end-user's personal data, but possibly also information on other people in the proximity. Yet, it is possible to process also context information legally, but a complex set of legal provisions need to be considered.

The *privacy and trust* function tends to provide technological solutions to privacy and trust problems. Very good. It seems, however, as discussed above that legal and other solutions must not be ignored either. On the other hand, a technology platform like this would be a most interesting target for malicious attackers. For instance, it would be very tempting for many people and companies to install into the system *spyware*, computer programs that covertly gather information on the end-user and delivers it to others. Spyware violates data protection law and may also constitute a criminal offence, but as the information can be extremely valuable, it is likely that there will be lots of attempts to use them.

The user interface *adaptation* function modifies both users' input modalities as well as services' output. It is also related to other adaptations, such as service quality adaptation. An important legal question here is related to copyright.

Copyright provides the copyright-owner with the exclusive right to modify the content. It is illegal especially to distribute adapted copyrighted content without permission. Many content owners (e.g. publishers and media conglomerates, but also individual artists and authors) are concerned about unauthorized adaptations for moral reasons, but also because they are afraid that poor adaptations spoil their valuable brands. A purely technical modification that does not affect the information content, but only data, is typically legal. That is, if changing the file format from one to another or a lossless compression has no affect whatsoever to the actual content, then the modification is alright. But if the modification changes notably the information, then it requires the copyright-owner's permission. If, for example, the resolution of an image of a valuable media character is reduced without permission to fit in a small display of a mobile device, it is likely that the copyright-owner will react. Therefore, it is important to make sure that the adaptation does not violate copyright.

There are three possible solutions to the problem. First, the service provider can use only content that is not copyrighted or in which the service provider itself has the copyright. This can be a feasible solution sometimes, but it depends on the business model. Second, it may be possible to get the consent of the copyright-owners for all the content in advance. Obviously, that also depends on the content and the business model. Third, it might be possible to interpret that the copyright-owner has actually given an implied consent and allowed necessary modifications when the content has been dis-

tributed. This is a very insecure interpretation and one should not rely on it in general.

Note that in some jurisdictions, e.g. in Finland, modification right is not a separate, independent right, but either part of distribution right (exclusive right to make the work available to the public, in either the original or an altered form) or moral rights (the work may not be altered in a manner that is prejudicial to the author's literary or artistic reputation or to his individuality). On the other hand, in the USA, for example, the owner of copyright has the exclusive right to prepare derivative works based upon the copyrighted work. Therefore, the details of the right to modify a work depend on the country.

Another concern about adapting content: many countries have nowadays laws that protect network operators from being liable for illegal content. These safe harbor rules usually require that the operator is only a mere conduit and does not alter the information. If an operator or another service provider begins to adapt content then the safe harbor rules possibly do not apply any longer and it may become liable also for illegal content at large.

The *service usage* and *service management* functions provide information about the services supports various forms of service triggering, and support the lifecycle of services. The complex set of services implies that the system as a whole can be distributed to a large extent. There are important legal cross-border issues related to a distributed system like those that implement MobiLife architecture. If a system is distributed in several countries, all the applicable laws should be obeyed. For example, transferring personal information even within the system but between organizations and/or countries may violate data protection law. Similar problems arise if MobiLife system is connected to other systems. So, both internal and external data processing should be legal. Also, data protection directives are implemented in slightly different ways and they are not applicable outside the EU. Thus there are differences e.g. which information is to be provided for data subjects, i.e. for those whose personal data is processed. These are pretty hard requirements for any system, but especially for systems like those implementing MobiLife architecture.

Liability questions in this kind of an environment can be complex. If an ad-hoc group of people is willingly sharing personal information, say context data, but something goes wrong and too much information is shared or some of the information is unwillingly disclosed to outsiders, it can be difficult to find out, who is responsible. First, it is difficult to show, who was actually doing something wrong, if it was, say, partly a technological failure, partly due to an incorrect configuration that the group members had created together. Second, according to European data protection law, the controller is largely liable, but in a dynamic ad-hoc group that distributes data more or less randomly between the members, it can be hard to call anybody ‘a controller’, unless the group as such is the controller. Likewise, if the group violates, for example, copyright law, it can be difficult to show, who is responsible, unless the whole group can be considered liable. An ad-hoc group, however, is hardly a legal entity and thus hardly liable in a legal sense.[9]

MobiLife service framework and its applications bring up several legal issues concluded below.

Privacy and Data Protection

Computing and communication devices are spreading everywhere in our society. In the future, those devices will become increasingly embedded in everyday objects and places, while communications networks connect the devices together and become available anywhere and anytime. This development is called ubiquitous computing (ubicomp), ambient intelligence (AmI), or pervasive computing. It can be seen partly as a parallel ongoing development with mobile technologies, partly as a successor to them. In any case, the tiny computing devices spreading everywhere will form the future technology environment of services. [2][3]

According to the European Commission’s Information Society Technologies’ Advisory Group (ISTAG): “in the physical world, domicile and residence are carefully developed and recognised concepts in terms of privacy and security protection in its broadest sense - legal, social, economic and technological. In contrast with the real world, there are few social and legal indicators of what constitutes a protected private space or an open public space in the virtual world. A comparable level of sophistication is needed in the future for people to feel at home within their smart homes,

with their online activities, and facilitate the personalisation of their everyday environment in order to enhance their mobility."[6]

How are ubicomp or AmI technologies going to affect privacy? It seems obvious that, because devices that are able to exchange information on people are spreading, the *quantity* of privacy problems will arise. The discussion above illustrates that very well. The framework includes a number of privacy issues. Although privacy problems are not that common today, it is predictable that they will be increasingly ordinary.

But will there be also something else? Will some *qualitative* changes also occur? At least three categories of qualitative transforms seem probable.

First, current legislation, although it claims to be technology neutral, is somewhat biased towards existing technical solutions, like personal computers, large displays, keyboards, and web pages. For example, according to the European Directive on privacy and electronic communications (2002/58/EC), services must provide continually the possibility, of using a simple means and free of charge, of temporarily refusing the processing of certain personal data for each connection to the network or for each transmission of a communication. It would be quite easy to fulfill such requirements with a PC based system, but very difficult with a tiny ubicomp device which has a minimal user interface.

Second, people's notion on privacy is changing. We are already getting used to the idea that while we are using for instance Internet services, someone can be able to observe our doings. While travelling abroad, we need to frequently present our passports and other documents, even though it makes it possible for authorities to follow our paths. In the past, that was not possible, but still most people are not concerned about the change. Either they accept the reduction of their privacy, because they think it is necessary or that they get something valuable instead, or they do not care. Anyway, it seems that most people will not object the gradual impairment of their privacy. In the future people will have a different notion on privacy and they will be happy with that.

Third, information and communication technologies will no longer affect only informational privacy, but increasingly also other sectors of privacy.

One well-known example is Professor KEVIN WARWICK who carries out research in artificial intelligence, control, robotics and biomedical engineering at the University of Reading. He has shown how the use of implant technology is rapidly diminishing the distance between humans and intelligent networks. In effect as a human is wired in to the network they become a part of that ambience themselves. This can have a tremendous impact in the treatment of different neural illnesses. There is a number of areas in which such technology has already had a profound effect, a key element being the need for a clear interface linking the human brain directly with a computer. [12]

Professor WARWICK's own research has led to him receiving a neural implant which linked his nervous system bi-directionally with the internet. With this in place neural signals were transmitted to various technological devices to directly control them, in some cases via the internet, and feedback to the brain was obtained from such as the fingertips of a robot hand, ultrasonic (extra) sensory input and neural signals directly from another human's nervous system. [12]

Professor WARWICK's shocking examples show how the technology can also be used to observe and control the human being through the computer networks from distance. It is possible to even affect his brain's decision-making process. [12]

Until now, the developing information and communication technology has threaten only informational privacy. Professor WARWICK's examples nevertheless clearly show that the emerging technologies are not that limited: they are also capable of jeopardizing the other components of privacy. This implies a major qualitative change in privacy problems.

Intellectual Property Rights and Digital Rights Management

Copyright will have a central role in the information society. Right to copy and distribute information products and services, that is, to benefit economically from them is based on copyright. Therefore, many business models will increasingly depend on copyright. Traditionally, the most important part of copyright has been the exclusive right to make copies. Currently, the situation is changing. The way computers, networks, and other digi-

tal devices work means that information is all the time copied and copied again. It is no longer essential or even possible to restrict copying, but to try to manage the access to information.

Also, as discussed above, the *adaptation* of content for various devices will become increasingly important issue. It is plausible that the focus within the copyright system will move from the exclusive right to make copies towards the right to modify the work. As noted above, international harmonization has not gone too far in this subject and therefore the details differ in different jurisdictions. If the right to modify a work becomes increasingly important, it is essential to study what would be the adequate legal approach from the services sciences viewpoint.

On the other hand, copyright also provides the author with moral rights: for many people, especially amateurs, it is not so vital to make money from the works they have created, but to get credited as an author. Therefore, copyright can be important also for non-profit communities.

Digital Rights Management (DRM) refers to copyright technical protection. Often, it is not enough that the law stipulates the rights of the copyright-owner. Especially, the content-industry has required technical tools that give them additional protection. DRM technologies are usually based on encryption: data is encrypted in a way that unauthorized access to information is difficult. A DRM system allows the end-user to access the information, e.g. listen to the piece of music, watch the video, or play a computer game, only in accordance with the license terms that are expressed in machine-readable rights expression language (REL). Obviously, the most important license term is usually that the end-user must pay for the usage in advance. Also, the license terms may restrict how many copies of the product the end-user may produce, and in how many devices those copies can be used.

DRM technologies cannot protect data completely. It is always possible to circumvent the protection. Sometimes the circumvention is difficult and requires special skills, sometimes it is very easy. Yet, the content industry has lobbied for anti-circumvention rules. In recent years, copyright law has been amended to include this legal protection for digital rights management.

Digital rights management is often considered to be harmful for consumers and other end-users. Yet, there are situations in which an ordinary person may benefit from DRM technologies. As described above, copyright protects also works by common people and non-profit communities. If they want to be sure that their moral rights are respected, they may apply some sort of light-weight DRM technologies that do not necessarily limit accessing the information, but make sure that the work is always attributed to the creators.

On the other hand, DRM technologies may also involve severe privacy problems. Although DRM is meant to ensure copyright protection, it often manages also information on end-users, their behaviour and preferences. Therefore, a DRM system should also comply with the data protection law.

Other intellectual property rights, including patents, trademarks, database sui generis right, and domain names will remain important, but it does not seem that their relative importance would grow remarkably. [8]

Contractual Relations and Consumer Protection

New information and communication technologies introduce new kinds of contractual challenges. For instance, while users are moving, they have many kinds of wireless devices, and their access points to networks 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 which will not be available in the near future.

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. The scenarios and applications based on MobiLife Service Framework depict a somewhat wild future world in which various applications and services are provided through networks by numerous providers. It will be challenging for a consumer to know which providers are trustworthy and with whom it is safe to transact. Consumer protection law will have a difficult but increasingly important role to increase consumers' trust and to enable business.

4 Conclusions

This analysis is based on only one service framework. Therefore it is probable that it does not reveal all the important legal topics that should be studied within services sciences. However, based on my previous extensive scenario analysis, I am quite confident that the legal topics discussed above are among the most significant. [8]

Several legal areas are important within the context of services sciences. Especially, *privacy and data protection law* is highlighted in the analysis of the framework. That is not surprising since MobiLife as a project emphasizes privacy, security and trust questions. Therefore it is natural that MobiLife scenarios also bring privacy issues out. However, also the scenarios from other projects [8] support the conclusion that privacy and data protection will be most important legal topics in relation to emerging services.

MobiLife service framework and applications underline issues related to personalization and adaptation. The user profiles are often personal data that need to be processed in accordance with privacy and data protection law. The collector of data needs to specify a purpose for which the data is collected. Personalization is probably an acceptable purpose, but the collector should be able to specify it. If data is collected for another purpose, they should not be further processed in an incompatible way with that purpose and no inadequate, irrelevant or excessive data in relation to the purpose must be processed. Therefore, one needs to be careful if personalization avails of data that is collected for other purposes and is related to identifiable people. Also, it must be taken care of that any major decisions are not made based on wrong or partial information.

Recent development, especially emerging ubiquitous computing and ambient intelligence technologies suggest that no longer only informational privacy is threaten by new technology, but also the other components of privacy, like physical, decisional, dispositional and proprietary privacy, are jeopardized. Another qualitative change in privacy is that people's notions and expectations are changing: people are gradually accepting some forms of lessening privacy.

Other important legal areas in the framework are intellectual property rights, especially copyright, and contracts. Content adaptation, especially, might violate copyright. The service framework emphasizes the adaptation of content based on the device properties, context, user preferences, and so on. Adaptation is useful and required by presented technical solutions. However, although details differ in different legal systems, a copyright-owner typically has an exclusive right to distribute modified content. If the content is copyrighted, then permission is needed to adapt it. A purely technical modification that does not affect the information content, but only data, is usually legal, but if the modification changes the information, then it requires the consent of the copyright-owner. That is, if changing the file format from one to another or lossless compression has no affect whatsoever to the actual content, then the modification is alright, but if, for example, the resolution of an image is reduced without permission to fit in a small display of a mobile device, it is likely to infringe copyright.

Also, as discussed above, altering content may cause that an operator or a service provider is no longer a mere conduit, safe harbor rules will not apply any more, and the operator or the service provider becomes liable for illegal content at large.

Digital rights management (DRM) or copyright technical protection poses issues in relation to both intellectual property law and data protection law. DRM systems are meant to prevent unauthorized copying and to control the usage of content in accordance with license terms and conditions. Thus their basic nature is related to intellectual property rights, especially copyright. New anti-circumvention laws protect those technical protection systems and make it illegal to circumvent them. However, DRM systems typically process user information. Usually they need to have data at least on who is allowed to access the information. Sometimes DRM systems also collect other information on users to give feedback to service and application providers and to improve their business. Unless that data are anonymized, it is personal data governed by data protection law.

To conclude, the most important legal topics that should be studied further are:

1) Privacy and data protection
    a) The challenges that the growing number of privacy issues – because of new technologies – pose to the privacy and data protection law.

b) The contradiction between technology biased laws and the services based on new technologies.

c) The changing notion of privacy and how it affects the legislation.

d) Implants and other technologies that not only gather information on us, but can actually affect us physically may require the area of law to be widened.

2) Intellectual property rights

a) Copyright, especially the changing focus from copying to modifying.

b) Digital rights management with respect to services.

3) Contracts

a) The adjustments that the contract law needs because of new technologies.

b) In business-to-consumer markets, the revisions that the consumer protection law needs.

About the Author

Olli Pitkänen holds a doctorate in information technology, a master's degree in software engineering, and a master's degree in laws. He has worked as a researcher and a teacher at Helsinki University of Technology and at Helsinki Institute for Information Technology HIIT for about thirteen years. (http://www.hiit.fi) In 1999-2001, he was a visiting scholar at University of California, Berkeley. His research interests include legal issues related to information and communication technologies (ICT). Prior to academia he worked as a software engineer in several companies. He has also practiced law at Opplex Attorneys-at-Law and at Puiro Snellman Åkerlund Attorneys-at-law.

References

[1] Acquisti, A., Grossklags, J. *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.

[2] Friedewald, M., Wright, D. Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5, Report on the Final Conference, Brussels, 21-22 March 2006.

[3] Gow, G. A. *Privacy and Ubiquitous Network Societies*. International Telecommunication Union, ITU Workshop on Ubiquitous Network Societies, Document UNS/05, 2005.

[4] Gutwirth, S., De Hert, P., Moscibroda, A., Schreurs, W. *The legal aspects of the SWAMI project*. In: Friedewald, M., Wright, D. Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5, Report on the Final Conference, Brussels, 21-22 March 2006.

[5] IBM: Services Sciences, Management and Engineering, http://www.research.ibm.com/ssme/

[6] IST Advisory Group. Ambient Intelligence: from vision to reality. For participation – in society & business. European Commission, Information Society Technologies. 2003.

[7] Lessig, L. *Code and Other Laws of Cyberspace*. Basic Books, 1999.

[8] Pitkänen, O. *Legal Challenges to Future Information Businesses*, HIIT Publications 2006-1, Helsinki Institute for Information Technology HIIT, 2006.

[9] Pitkänen, O. Legal and Regulation Framework Specification: Competence within Mobile Families and Ad-hoc Communities, IST-2004-511607 MobiLife, D11 (D1.6) v1.0, 2006.

[10] Reuters, published on ZDNet News, http://news.zdnet.com/, March 31, 2003.

[11] Räisänen, V., Karasti, O., Steglich, S., Mrohs, B., Räck, C., Del Rosso, C., Saridakis, T., Kellerer, W., Tarlano, A., Bataille, F., Mamelli, A., Boussard, M., Andreetto, A., Hölttä, P., D'Onofrio, G., Floreen, P., Przybilski, M. *Basic Reference Model for Service Provisioning and General Guidelines*. IST-2004-511607 MobiLife, D34b (D5.1b) 1.0, 2006.

[12] Warwick, K. *Wiring in Humans. Advantages and problems as humans become part of the machine network via implants*. Presentation. Summary in Friedewald, Michael – Wright, David. Safeguards in a World of Ambient Intelligence (SWAMI), Deliverable D5, Report on the Final Conference, Brussels, 21-22 March 2006.