FIDIS

Future of Identity in the Information Society

Title:	D11.12: Mobile Marketing in the Perspective of Identity, Privacy and Transparency
Author:	WP11
Editor:	André Deuker (JWG)
Reviewers:	Mark Gasson (Reading)
	Mireille Hildebrandt (VUB)
Identifier:	D11.12
Type:	Report
Version:	0.8
Date:	Tuesday, 30th June 2009
Status:	[Final]
Class:	[Public]
File:	fidis-wp11-del11 12_mobile_marketing_20090630_final.doc

Summary

Deliverable D11.12 on Mobile Marketing in the Perspective of Identity, Privacy, and Transparency puts a multifaceted FIDIS view on the topic of mobile marketing.

Thereby the deliverable stresses on the role and importance of collecting information about users' identity attributes and their behaviour, as well as on the aggregation of identity information and external information such as geo data.

Legal foundations of mobile marketing are described on a European and national level. Methods on how to design parts of the mobile marketing process in a more privacy respecting and transparent way are proposed and conflicting interests within this process are addressed.

A summary and a list of topics to be researched in future concludes the deliverable.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	20.12.2008	• Initial set up of the document
0.2	26.03.2009	• First compiled version of the document
0.3	14.04.2009	• Elaboration of results of the 4th Work Shop on Mobility and Identity held in conjunction with the FIDIS General Meeting 2009 @ Frankfurt
0.4	05.06.2009	• Restructuration of chapters 3 and 4
0.5	16.06.2009	• Compilation of first review-ready version of the deliverable.
0.6	22.06.2009	• Consolidated post review version for revision by the chapter authors
0.7	27.06.2009	• Integration of revised chapters, reshaping of executive summary, introduction and conclusion taking reviewers' comments into account.
0.8	30.06.2009	• Finalisation of the deliverable

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive Summary	André Deuker (JWG) Kai Rannenberg (JWG)
2 Introduction	André Deuker (JWG)
3 Database Marketing and Data Mining	Sandra Steinbrecher (TUD), Stefanie Poetzsch (TUD)
4 Recommender systems for mobile marketing	Mike Radmacher (JWG)
5 Requirements for legal compliance and legal safeguards for transparency in mobile marketing	Harald Zwingelberg (ICPP), Maren Raguse (ICPP)
6 Country Report Germany	Harald Zwingelberg (ICPP), Maren Raguse (ICPP)
7 Country Report France	Fanny Coudert (KU LEUVEN)
8 Intellectual Rights as Obstacles for the Transparency of Profiling Processes	Niels van Dijk (VUB)
9 Conclusion	André Deuker (JWG) Kai Rannenberg (JWG) Harald Zwingelberg (ICPP)

Table of Contents

1 Executive Summary

Within the last two decades mobile devices have made their way towards being a ubiquitous item in private, social, and professional life. Services designed for mobile usage benefit from the attributes of mobile communication e.g. the knowledge of users' current positions and further context information. To a large degree, this is enabled by the underlying identity management (IdM) structures of mobile operators, which were originally set up for accounting purposes.

Meanwhile the business models of mobile services got under pressure: classical revenue models are not appropriate in many cases, e.g. due to the commoditisation of mobile voice telephony, that lead to a sharp decline in revenue. New revenue models, e.g. based on the concept of mobile marketing, can help with offering mobile services while yielding a sufficient profit. The large amount of context information available in mobile networks is a unique feature, distinguishing mobile marketing from all competing advertisement channels, such as print media, television, or fixed line Internet. Nonetheless, the availability and active use of customers' time, locality, interest, and action specific context implies that misuse of collected data can happen and that users' privacy is at stake. Data of someone using location based services are continuously and pervasively collected and can become used for increasingly specialised and personalised marketing offers. The person in question will be barely aware of these ubiquitous underlying profiling processes. Therefore the deliverable at hand focuses on the role of identity attributes in mobile marketing, and especially on aspects of privacy and transparency of mobile marketing business processes.

Knowing about users' interests, behavioural patterns, and attitudes towards incentives is a necessity for customising services in an efficient way. This also holds true for mobile marketing. Therefore the process of extracting customer characteristics is discussed and a technical method for privacy preserving data mining is presented. On the application level the deliverable presents an approach how transparency in mobile marketing applications can be established, and what benefits potentially come along with it.

Besides this technical and economic driven view on transparency in mobile marketing the report stresses on transparency as a legal obligation for mobile marketing applications. In particular the transparency principle is examined in its legal grounds in the data protection legislation on European as well as on national levels in Germany and France. Transparency is a central element of the European framework on data protection and privacy. Data subjects have the right to be informed about the identity of the controller, the purposes of the processing for which the data are intended and possible recipients at different stages of the processing of the data. In the last chapter we will assess how these conflicting rights and interests might be balanced by analysing legislative proposals and jurisprudence.

Although several aspects affecting users' identity could be addressed, we see that further research needs to take place to adapt technical mechanisms and legal safeguards in a way that allows preserving users' identity and respecting providers' claim on intellectual rights.

2 Introduction

In the course of the last two decades, the evolution of the information society was closely connected to and supported by the evolution of the mobile communications industry. Rapidly, mobile devices appeared in the bags and pockets of more and more people. In the following years, mobile devices made their way towards a ubiquitous item in private, social, and professional life. Mobile communications means the ability to access information networks or to use communication tools independent of the location. In addition, mobile communications allows for an explicit consideration of users' current positions and further context information in the process of service creation and provisioning. To a large degree, this is enabled by the underlying identity management (IdM) structures of mobile operators, which were originally set up for accounting purposes.

The relation between users and their devices is most often a very personal one, comparable to their bunch of keys or other personal items. Although the purpose of the subscriber identity module (SIM) still is the identification of accounts, this identification is not necessarily restricted to accounting purposes alone. It is also possible to use the SIM card for establishing links to more sophisticated profiles, compared to the original accounting driven profiles of mobile operators. This new type of profile can be stored at locations, different from the accounting profile of the mobile operator. To this regard, the control of these profiles is shifting to more and different parties. Depending on the positioning technology used and the set up for the profile's underlying service, the mobile operator can even be excluded from the process of providing context aware services besides his function as identifying party and communication channel.

Looking at the underlying business models of mobile services, classical revenue models as central parts of the business model are not appropriate in many cases. Although customers consider context aware services as being useful in principle, their willingness to pay for a concrete service is most often lower than the actual costs of developing and providing the service. New revenue models, e.g. based on the concept of mobile marketing, can help in offering these services while yielding a sufficient profit.

Mobile marketing as a basic concept for these new revenue models is characterised by the enrichment of classical marketing methods with mobile communications technologies. From a commercial perspective, the ability to identify and address individual customers, the availability of users' context information and the possibility to receive immediate customer response are key features that distinguish mobile marketing from other marketing set-ups. A large number of mobile marketing definitions have been published and discussed in the literature. The purpose of this deliverable is not to derive new definitions or to discuss present ones. Nonetheless, from a FIDIS project perspective the following properties of mobile marketing should be highlighted:

> *Mobile marketing is interactive, context sensitive (including location), personalised, wireless and has the goal to promote goods and services.*

This working definition is based on the definitions by Dickinger and Haghirian that among other mobile marketing definitions can be found in (Leppäniemi, 2006).

Information about users' identity is collected and processed on different levels within the process of creating individualised marketing contents.

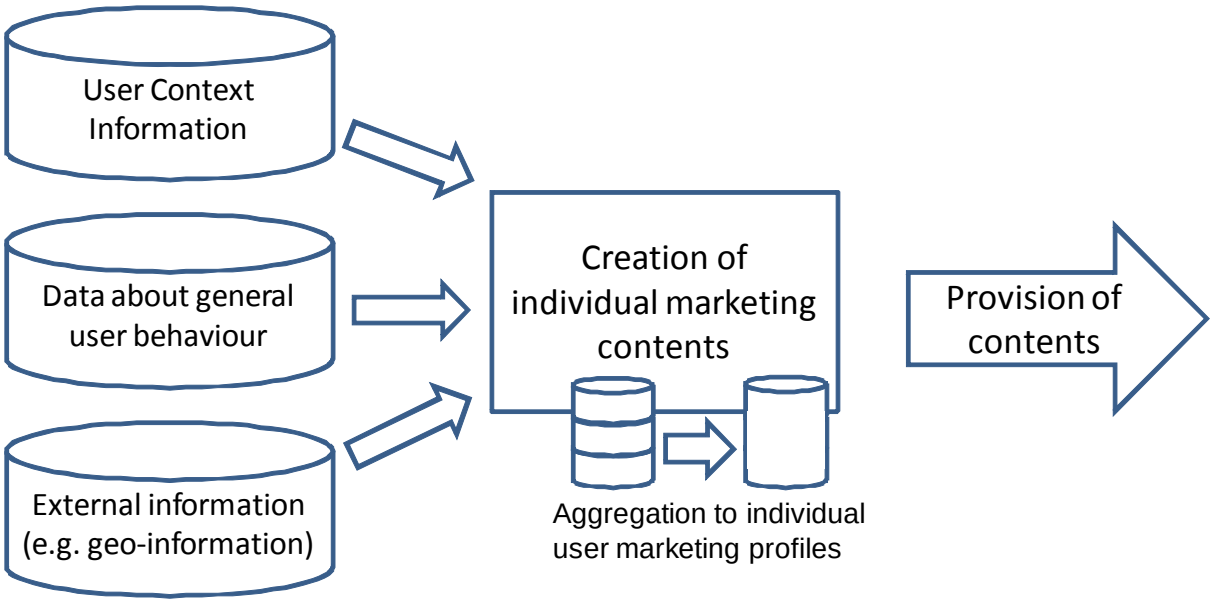

Figure 1 Collection and aggregation of identities

The collection of information about users' identity (user context information) and the ability to address them directly represents a prerequisite for individualisation in mobile marketing. In addition to that information about users' identity are collected and pooled in order to gain general data and knowledge about their behaviour and interests. According to the classification of Durand different types of an individual's identities are matched in a profile used to create mobile marketing contents. This may take place without the users' are even knowing about it.

Mobile marketing, as it has been briefly described and defined above, has many facets that relate to topics discussed in FIDIS. Based on the results of the overall network and in particular on the outcomes of Work Package 7 on profiling and Work Package 11 on mobility, the present deliverable D11.12 will focus on the role of identities, privacy, and transparency in mobile marketing. From a technical perspective, D11.12 is based on the following FIDIS deliverables, which the reader is encouraged to view:

- D3.3: Study on Mobile Identity Management,
- D7.2: Descriptive analysis and inventory of profiling practices,
- D7.3: Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence
- D11.2: Mobility and LBS.

Legal and economic aspects laid out in this deliverables are also based on a number of work package 7 and 11 deliverables, those are:

- D7.7: RFID, Profiling, and AmI
- D7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools
- D7.16: Profiling in Financial Institutions
- D11.3: Economic aspects of mobility and identity and
- D11.5: The legal framework for location-based services in Europe.

The goal of D11.12 is to deliver a domain specific concretisation and extension of results presented in (at least some) of the listed deliverables.

The large amount of available context information in mobile applications are a unique feature, distinguishing mobile marketing from all competing advertisement channels, such as print media, television, or fixed line Internet. Nonetheless, the availability and active use of customers' time, locality, interest, and action specific context implies that misuse of collected data can happen and that users' privacy is at stake.

The degree of privacy enforcement, understood as an active decision of customers' to disclose or conceal certain attributes of their identity has implications for the quality and the creation of value for all involved parties. The example of the mobile recommender system in Chapter 4, a typical mobile marketing application, gives a glimpse of how users' trade-off between disclosing and concealing identity information could look like. On the one hand the availability of additional customer metrics leads to better recommendations, thereby reducing customers' search cost. On the other hand this keeps the danger of privacy invasion and wrong conclusions.

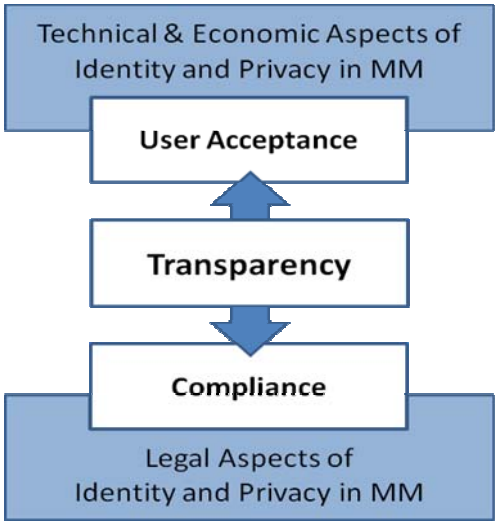

Figure 2 Scope of the Deliverable

Disclosing personal information to a provider is always a matter of trust. The concept of trust of course is a very strong and broad one, but most authors agree on transparency and control as two major pillars of the concept. Focussing on the aspect of transparency this deliverable presents two concepts in the area of mobile marketing that have the potential to raise users' acceptance of mobile marketing applications, namely privacy preserving data mining and transparent design of mobile recommendations. This will be further elaborated in Chapters 3 and 4. We hypothise that the active creation of trustworthiness and the enhancement of users' privacy will raise acceptance of mobile marketing applications.

Another aspect this deliverable aims to contribute is the examination of the role of transparency in mobile marketing from a legal standpoint. Legal foundations of mobile marketing will be examined in Chapter 5 on a European and more concretly on national level for Germany and France in Chapters 6 and 7. Chapter 8 focuses on the application of transparency enhancing technologies and discusses the trade-off between users' right to

access and control data on the one hand and intelectual property rights of service providers on the other hand.

3 Database Marketing and data mining

With the onset of the information society and the emergence of the information flow, the user is confronted with the conflict between getting the information he is looking for and spending the time he is able to, while searching for what he is interested in (Bleicher and Hickethier, 2002; G. Franck, 1998). "To give customers exactly what they want, you first have to learn what that is. It sounds simple, but it's not" (Zipkin, 2001). It implies that information about customers needs to be collected. Technically information can be collected and stored in databases. Then database marketing can be applied as a form of direct marketing to start the process of creating and communicating personalised offerings for (potential) customers. For communication different methods can be used. Directly addressing the (potential) customers by personal contact, phone calls or e-mails is the direct and obvious way. Other methods like embedding personalised advertisements in a website or in our physical environment often are not recognised as personalised marketing directly by the (potential) customers addressed. While some years ago in the physical environment advertisements could not be designed in a personalised way nowadays and in the future with the methods of ubiquitous computing this becomes possible (Radmacher, 2008a; Radmacher, 2008b).

Database marketing makes use of data mining and (new) knowledge discovery to develop models of customer behaviour. These models abstract from the concrete customer but try to classify customers and products in classes and identify rules for behaviour in different classes. The rules are used to select both customers to be addressed and products to address customers with. Data mining and knowledge discovery techniques need as much data as possible about customers to increase the probability that the model developed fits the needs.

The data for such a database may, for example, be collected from details of the transaction history with one's own customers or bought from third party companies that have captured the information. Typical sources of compiled lists are charity donation forms, application forms for any free product or contest, product warranty cards, subscription forms, customer loyalty programs, and credit application forms. Data of interest and collected for so-called customer profiles can be manifold, starting from name and address, history of shop searches and purchases, demographics, and the history of past communications to and from customers.

3.1 Data mining - how it works

Data mining[4] is usually done in the following way (Berson *et al*, 1999):

First from raw data to use from different databases for data mining has to be selected and then extracted. Then the data extracted has to be prepared by e.g., deleting redundancies, making synonyms consistent and possibly also by anonymising data if this has not been done by the providers of the databases.

Then a **model for classification of records** has to be developed. Clustering and the Nearest Neighbour prediction technique are very old techniques used in data mining for clustering. Clustering means records are grouped or clustered together. A subset of attributes of every record can be used to decide to which class a record should belong. A possible example for an insurance company might be "Every car driver under the age of 25 has a high risk for causing

[4] More research on data mining techniques had been done in FIDIS in work package 7. For further details we refer in particular to the FIDIS deliverables D7.2 pages 26 et.seq. and 83 et.seq. and D7.3. Decision trees had been described in in FIDIS deliverable D7.2 pages 29, 84. See chapters x and x in Hildebrandt, M. and S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspective, Dordrecht Springer 2008.

accidents". All other attributes might not be of interest if the attribute age is under 25. Nearest neighbour is a prediction technique that is quite similar to clustering - its essence is that in order to predict what a prediction value is in one record look for records with similar predictor values in the historical database and use the prediction value from the record that is "nearest" to the unclassified record.

More sophisticated techniques have been developed that can be used for either discovering new information within large databases or for building predictive models. Among them are decision trees, neural networks and rule induction.

1. In a decision tree the possible attributes of data records are modelled as branches of the tree to give a predictive model of customer behaviour. Each branch of the tree is a classification question of attribute values and the leaves of the tree are partitions of the dataset with their classification.
2. Neural networks create very complex models that are almost always impossible to fully understand even by experts. The model itself is represented by numeric values in a complex calculation that requires all of the predictor values to be in the form of a number. The output of the neural network is also numeric and needs to be translated if the actual prediction value is categorical.
3. Rule induction on a database often has to test many possible patterns of data. To every pattern an accuracy and significance are added to indicate its strength and the likelihood to occur again. In general these rules are relatively simple such:For a market basket database of items scanned in a consumer market basket you might find interesting correlations in the database. Internet shops demonstrate this every day by presenting items to us on personalised website that other users with the same purchases than ours bought.

3.2 Privacy in data mining

Although the goal of data mining algorithms is to move from individual raw data to general data that can be applied to classes of people, privacy issues are still important. From the privacy perspective the large customer profiles that can be built with the help of large databases should be protected. But it is very difficult to define what privacy means for data mining. According to (Vaidya *et al*, 2006) "a privacy-preserving data mining technique must ensure that any information disclosed

1. cannot be traced to an individual; or
2. does not constitute an intrusion."

For the first requirement identifying data have to be removed in the preparation of data for the data mining algorithm. For anonymising data records contained in a database, not only obvious identifiers such as name, national ID number, or address have to be removed. Often, if no further precautions are taken when releasing the data, the remaining attributes may constitute an identifier, or quasi-identifier, that allow for re-identification of the data subject when combined with other sources of information (e.g., publicly available information like statistical data). The so-called *k*-anonymity (Sweeney, 2005) proposes a method to generalise attribute values, such that each possible query consisting of a combination of attribute values gives as result a set of at least *k* records. More details on privacy metrics can be found in FIDIS Deliverable 13.1.

The second requirement is very difficult to decide on because data mining as marketing technique has the goal to find out what has "value for (potential) customers". And deciding on value for others might "constitute an intrusion" into their private sphere.

Beneath privacy transparency for the user, disclosing which data are collected and what these data are used for is important. More details about this will be explained in section 5 for recommender systems that user the databases collected and processed by data mining algorithms.

3.3 Privacy-preserving data mining techniques

At least in the research community a lot of research is done on privacy-preserving alternatives for existing data mining techniques. In this section we provide an overview on the state-of-the-art in privacy preserving data mining as an extension of (Verykios *et al*, 2004). There privacy marketing is classified based on the following dimensions:

1. **Data distribution:** Data needed can be stored
    1. centralised or
    2. distributed. Distributed storage can be classified again in horizontal (database records are at different places, but every record is complete) and vertical (different attributes in different places, but at no place is a complete record) storage.

- **Data modification:** The data stored has to be modified before being released to ensure the privacy of the customers concerned.
    - Perturbation: An attribute value is altered to a new value (i.e., adding noise).
    - Blocking: Certain attributes are not published, but substituted by "not usable".
    - Aggregation: Information about a set of data shall be retained, but the value of single attributes should be hidden. This means a set of values is grouped as the same category.
    - Swapping: Two values of two data sets are changed.
    - Sampling: The database is not used as a whole but only a sample of a population.
    - **Data mining algorithm:** Some examples are decision tree inducers, clustering algorithms, Bayesian networks.

- **Data or rule hiding:** Both raw data and aggregated data can be hidden. Due to the fact that hiding aggregated data in the form of rules is more complex mostly heuristics are used.
- **Privacy preserving data mining technique:** Techniques that are used so far are:
    - heuristic-based techniques that modify only selected values to minimise the utility loss.
    - calculation on encrypted data (secure multi party computation) does not allow any party participating in the calculation to learn anything except its own input and the data mining results.
    - reconstruction-based techniques try to reconstruct the original data distribution from randomised data at an aggregate level.

3.4 Examples of privacy-preserving data mining techniques

Reconstruction-based techniques:

An example for a privacy-preserving decision tree classification for numerical data is presented in (Agrawal and Srikant, 2000). The algorithm uses known training data that has already been classified. To the training data, perturbation has been applied. They give the following Bayesian-based reconstruction approaches to build the decision trees:

1. global: For every attribute the distribution of values is reconstructed separately and based on this the decision tree is built.
2. class-based: additionally to the global approach, for every class the distribution of values is reconstructed separately and based on this the decision tree is built.
3. local: additionally to the class-based approach when building the decision tree for every node the distribution of values is reconstructed.

Calculation on encrypted data:

The definition of privacy for secure-multi party computation is that the calculation is private as long as none of the parties involved knows more than her input and the result of the calculation. It is quite clear that then every party involved in the calculation only has a part of the available data. For the storage of data this means that it is distributed. For both horizontal and vertical storage, protocols have been proposed as described in (Verykios *et al*, 2004). But the crucial point for secure multi-party computation is that it is often very inefficient because all calculations to be done need the homomorphism of the encryption.

3.5 Private information retrieval and other user-controlled alternatives

Private Information retrieval (Chor *et al*, 1995) allows users to request data from a database in such a way that the provider of the database does not get to know the concrete data records of the respective information a user is interested in. The security of PIR depends on its concrete implementation:

The only possible protocol that offers the end-users unconditional unlinkability of the data requested of him is the request of the whole database. For a more efficient solution there are two possibilities: Either the computation power of the database provider can be assumed to be computationally limited or it has to be assumed there are non-cooperating providers that all hold a copy of the database. There exist numerous PIR protocols and studies on how efficient PIR can become when assuming different computational boundaries of the database providers.

While the providers do not get to know what "has value for a customer" the end-users have to find out such offers themselves and ask for offers of these products. For this reason PIR is of no interest for marketing applications.

Another user-controlled alternative to classical data mining is to give end-users the possibility to do data mining themselves by giving them access to databases and providing them with the respective data mining algorithms. But data mining algorithms often are of high value for

marketing strategies and should not be shared with others. If the user gets neither access to data nor to the data mining algorithms from the marketing perspective privacy-preserving data mining is the only possible compromise between marketing wishes and end-users' demand for privacy.

3.6 Data mining in mobile applications

Data available for providers of any kind of mobile or geographic services reveals even more about their users' physical life than data just collected by classical Internet services. More and more marketing activities explicitly address people's physical places and begin to integrate advertisements in their physical life. This becomes even truer for ubiquitous computing when users do not interact with the computing infrastructure explicitly and may not even be aware of marketing activities.

Marketing activities also affect users' physical life by distributing the personal data contained in advertisements (e.g. shop offers based on past purchases) from the home personal computer in former days to the places users surf in the Internet. Thereby everyone sitting near to such users is able to learn a lot about others' behaviour. And by misleading rules used for data mining also false conclusions about users can be drawn.

4 Recommender systems for mobile marketing

The contribution of this section is mainly based on Radmacher (Radmacher, 2008a; Radmacher, 2008b) Recommender systems gain significant importance by helping the user to find what he is actually looking for, as e.g. service providers which are "suggesting … those products which best suit his needs and preferences in a particular situation and context" (Nguyen and Ricci, 2004). The databases needed for recommender systems can in principal be built by every data mining techniques explained in section 3 including the privacy-respecting ones. Nevertheless for giving recommendations to concrete, but possibly pseudonymous customers, at least pseudonymous profiles for these users have to be built. Here privacy-respecting data mining will not work because the customer needs to be addressed and thus profiling exactly him is required. Nevertheless for the common database used for recommendations privacy-respecting data mining techniques can be used.

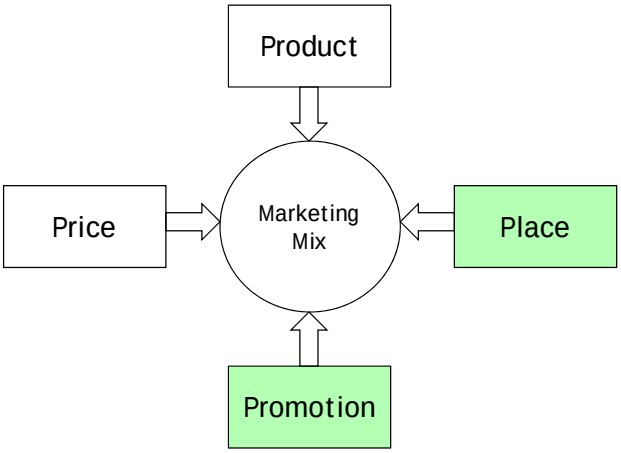

Figure 3 Recommender Systems and Marketing

From a marketing perspective recommender systems work as the place and promotion functions of the classical marketing mix (4 P's – product, place, promotion and price). The place represents the location where a product can be purchased. It is referred to the distribution channel. The promotion represents the act of getting in touch with the potential customer. In this case mobile recommendations are used as distribution channel in e.g. a virtual shop, the place where products are purchased but also are promoted as long as customers' preferences are focused.

The idea of recommender systems is not new and a lot of systems are well known in academia as well as in practice. GroupLense (Konstan *et al*., 1997), MovieLense (Dahlen *et al*., 1998), Video Recommender (Hill *et al*. 1995), Ringo (Shardanand and Maes) and Fab (Balabanović and Shoham, 1997) are only a few systems that are developed by researchers in order to understand and optimise current recommendation processes. Some websites like Amazon.com, CDNow.com, Barnes & Nobel, MovieFinder.com, Pandora.com, TiVo.com, Netlix.com or Launch.com have made successful use of recommender systems (Hingston, 2006; Herlocker *et al*. 2002; Sinha and Swearingen, 2002).

Research in the area of recommender systems has been performed over the last 20 years in a few different areas. The algorithm refinement, the analysis of user behaviour and the consideration of user feedback are typically distinguished. Algorithm refinement is conducted on the one hand by optimising recommender techniques like rule-based filtering, content-based filtering, collaborative filtering and hybrid approaches (Balabanović and Shoham,

1997; van Meteren and van Someren, 2000; Eui-Hong and Karypis, 2005; Sarwar *et al*., 2001; Linden *et al*., 2003) and on the other hand by addressing new application areas with specific domain related input vector e.g. music (Donaldson, 2007) or video (Konstan *et al*., 1997; Dahlen *et al*., 1998). The analysis of user behaviour is accomplished by classical research separated into the active way which asks the user explicitly about his behaviour (Jung *et al*., 2007) and the passive way (Fu, 2007; Kelly and Teevan, 2003) where the behaviour is derived by indirect information collection and interpretation. The third path of research in recommender systems addresses the consideration of user feedback, often given by the buzzword "recommendation by critique" (Nguyen and Ricci, 2004; Ricci and Nguyen, 2004; Pu, 2003). All these topics are of importance but for a while researchers have recognised that something different is coming up.

4.1 Missing Trust

When using recommender systems users typically disclose some personal opinions e.g. in the form of ratings. Based on these ratings a recommendation e.g. for movies, books other products is made. The user has the possibility to accept or reject the recommendation. Over the years literature have indicated that recommender systems are not always trusted by users (Herlocker *et al*., 2002; Sinha and Swearingen, 2002; Swearingen and Sinha, 2001). Most of the recommender systems act as black boxes, not offering any insight into the systems logic or justifications for recommendations and cannot be questioned (Herlocker *et al*., 2002; Sinha and Swearingen, 2002; Swearingen and Sinha, 2001). Recommendations are often correct, but also occasionally very wrong (Herlocker *et al*., 2002). There are no indicators given when to trust a recommendation and when to doubt one from the users' point of view (Herlocker *et al*., 2002). In addition, a user is very sensible when it comes to recommendations in an area he is not familiar with (Sinha and Swearingen, 2002).

Moreover there is a huge difference when talking about recommendations between humans & computers and humans & humans. A recommendation process between humans typically looks like this (Herlocker *et al*., 2002): When you decide to accept a recommendation from a friend, it involves the consideration of the recommendation's quality. You compare how that friend's general interests correspond with your own in the domain of the suggestion. You probably ask yourself if the recommendation makes sense to you. If there is any doubt, you will ask your friend why he has made this recommendation. Your friend will explain his reasoning behind his suggestion. You can analyse the logic of this suggestion and determine yourself if the evidence is strong enough. In the end you accept or disregard the recommendation.

This possibility of scrutinising a recommendation is not given today. Transparency can help (Hingston, 2006; Herlocker *et al*., 2002; Sinha and Swearingen, 2002; Tintarev and Masthoff, 2007; Tintarev, 2007). Transparency is about explaining to the user why a particular recommendation was made (Herlocker *et al*., 2002; Tintarev and Masthoff, 2007; Tintarev, 2007). It explains how a system works (Tintarev, 2007; Muramatsu and Pratt, 2001), enables the user to make a more accurate judgment of the true quality of a recommended item (Bilgic and Mooney, 2005). Transparency can increase the trust of a system (Herlocker *et al*., 2002; Sinha and Swearingen, 2002; Swearingen and Sinha, 2001; Awad and Krishnan, 2006), offer a higher acceptance of recommendations and can increase sales, communicated by transparent recommendations (Sinha and Swearingen, 2002).

Transparency is even more important in a mobile environment because personal information e.g. location, time of usage, interests, and other situational dependent information can be used

in order to offer a more individualised recommendation (Figge, 2007; Albers, 2007). Processing this information especially location information mostly needs users' approval (Radmacher *et al*., 2007; Zibuschka *et al*., 2007). Transparency, for instance, can be used for building trust and to enable a way of checking if personal privacy policies are respected. Furthermore transparency of mobile devices needs a completely different way of visualisation and interaction with reference to its limitations (Radmacher, 2007b).

4.2 The Definition of Transparency

The aim of transparency as part of current research activities is about increasing customers' trust in the relationship between the customer himself and a service provider who is offering personalised recommendations. Furthermore the tolerance against wrong recommendations should be increased, too. The idea of increasing customers' tolerance is about explaining to the customer why a recommendation went wrong and offering the possibility to critique the explanation. This will hopefully lead to direct customer feedback that can be used to optimise current and future recommendations. Critiquing gives the custumer the opportunity to get an idea of how the recommendation was generated, in detail the customer is able to understand what kind of personal information is used in order to create this recommendation. If a customer does not understand why a recommendation went wrong, he will use another recommender engine instead of using the same recommender engine again. One would thus expect that the customer retention rate will increase if transparency is realised. The underlying research question is: (RQ1) How can transparency be defined (e.g. characteristics) and realised (e.g. design elements) in a mobile environment by considering its advantages and limitations? RQ1 addresses the definition itself and visualisation aspects related to the assumption that transparency can be given through explanations. According to design research, the following artefact has to be designed: By addressing RQ1 the concept of transparency for a mobile environment is defined that includes the consideration of questions from a data processing point of view.

The contribution of this section is focused on mobile recommender systems based on the following wherefores. Since 1990 a rapid growth of mobile communication which changed the way of communication is noticed. In 2008 we had 100 Million mobile contracts in Europe. Furthermore in a mobile domain more personal information (e.g. location, time, interests, action-based information) of users can be used in order to offer a more individualised recommendation. Addressing the customer in a more individualised manner works as an enabler for mobile marketing activities (e.g. advertisement based revenue models). Mobile recommender systems help to reach the right customer at the right point in time and place in order to offer the right product but recommendations on mobile devices need a completely different way of visualisation and interaction with reference to its limitations.

When you start thinking about how a mobile recommendation can be made transparent from a user's point of view, at first it is important to know what transparency is about.

Figure 4 illustrates how transparency can be defined, separated into characteristics and functions. Most of the characteristics are self-explanatory as visible (Koenemann and Belkin, 1991), understandable (Maaß, 1994), self-explanatory (Sinha, and Swearingen, 2002; Wandmacher, 1993), interactive (Tintarev and Masthoff, 2007), transparent (Bodker, 1987; Norman, 1998), traceable (Fritter, 1979), controllable (Frese, 1987) or penetrable (Spinas *et al*., 1983; Oberquelle, 1994). The functions that transparency enables or supports allow the customer to make a more accurate judgment of the true quality of a recommended item

(Bilgic and Mooney, 2005), mechanisms for error handling (Herlocker *et al*., 2002), explanations why a particularly recommendation is made (Sinha, and Swearingen, 2002; Tintarev and Masthoff, 2007; Swearingen and Sinha, 2001), explanations on how the systems works (Tintarev, 2007; Muramatsu and Pratt, 2001; Maaß, 1983), provisioning of information and processes [30] and insights into information that a firm stored about a user (Awad and Krishnan, 2006).

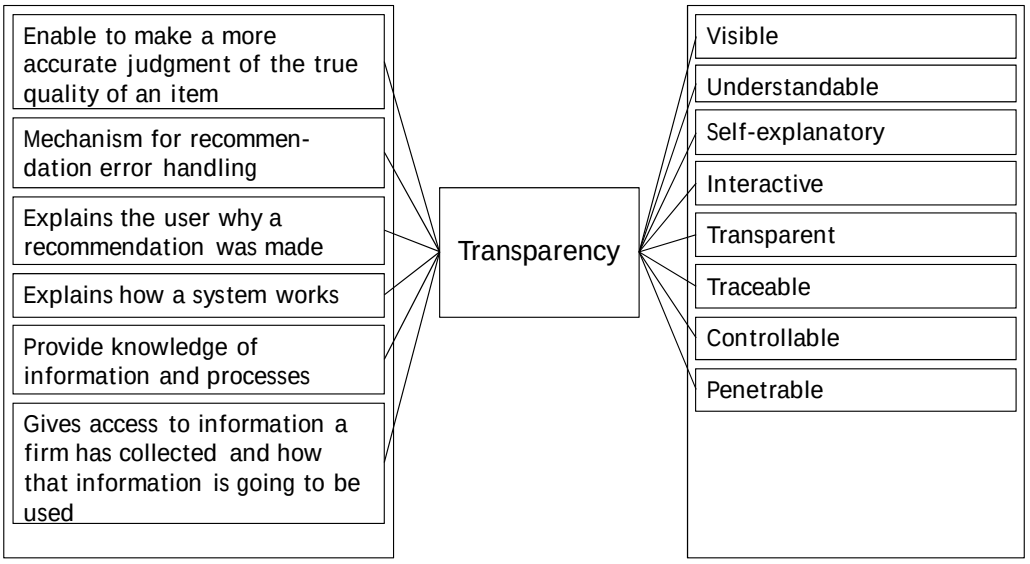

Figure 4 How is transparency defined?

When it comes to transparency, there are less research results available with reference to recommendations as well as mobile recommendations. Two studies (Movielens and LIBRA) are known that address research on transparency. One is conducted within a project called Movielens. The aim of this project was to identify a visualisation form that leads customers to buy a product with a higher probability. A survey was conducted with 78 participants and 21 different visualisations. A collaborative filtering mechanism was given as a starting position. While the aim of the survey sounded promising, the results were very limited. As a result the survey identified a histogram as the best way to present recommendations to the customer. Aspects of transparency as described in this article were not focused. Mobile aspects were not part of the survey. The second study called the LIBRA project was about the idea that satisfaction is more important than promotion. A good and transparent recommendation not only convinces the customer to buy a product, it also discloses the products quality and benefits. The study analysed three different visualisation forms for 3 different methods and asked 34 participants. The results were promising even if they were general. The study indicated that explanation for a recommendation should not include any technical or statistical description within an explanation; text and diagrams are the favourites and it seems that an explanation has a direct influence on the customers' buying behaviour. Critique regarding the survey is about the limited amount of participants, only 34, about the more general statements and about not focusing on the mobile environment. However, in total the survey shows to some degree the importance of transparency within recommendations.

4.3 Visualisation of Transparent Recommendations

Therefore Radmacher (Radmacher, 2008a; Radmacher, 2008b) set up a survey that allows to understand how important transparency is and more important how can I visualise transparent mobile recommendations. The conducted survey supports RQ1 by indicating what kind of design component might be appropriate from a users' point of view. Based on the construction of a second artefact the systematic and engineering course of action to develop and integrate a software component that enables transparency within mobile recommendations can be initiated. Derived hypotheses to support RQ1 are the following:

(H1) Recommender systems are used and helpful in the users' daily life.

H1 is based on the assumption that people who realised the usefulness of recommender systems, used them a lot and maybe different ones. Therefore they will recognise differences in the visualisation.

(H2) The relevance of transparency is more important for those who know that personal information is processed within recommendations.

People who know that a lot of personal information is saved and exchanged are more interested in the nature of recommendations (the information that is used to generate a recommendation) than people who are not aware of the information collection.

(H3) The combination of text and icons as a style element is the best solution to visualise transparent mobile event recommendations on a mobile device.

Based on the history of mobile navigation menus it is assumed that the combination of text and icons might be the best way to visualise an explanation for a recommendation in an area the user is not familiar with.

(H4) Three explanations for one mobile event recommendation are sufficient to offer transparency from users' perspective.

H4 is based on the assumption that a mobile display is limited in size. If an explanation contains text and icons maybe three or four explanations will fit on a display without scrolling.

While H1 and H2 have a more general character to support the motivation, H3 and H4 support the design aspects for transparency.

To examine the hypotheses described above, a survey was conducted. Test subjects were volunteer users (n = 318) who are technical affine. In addition they also have a mobile device, use it often, even if they did not use mobile recommender systems, and they are aware of their limitations. All participants reported by using the internet. The survey consists of 4 different sections. Section A is about general statistical questions as age, gender, family status and occupational category. Section B of the survey asked about the personal relevance of recommender systems (e.g. usage or usefulness) on the fixed as well as on the mobile internet. Both sections help to confirm if the right target was met as well as to answer H1 and H2. Section C of the survey is about transparency in recommender systems. The test subjects were asked if they know that personal information can be processed in order to generate recommendations. Furthermore, they were asked if they know what kind of personal information is processed. In addition, questions about the understandability of today's recommender systems, its visualisation as well as its transparency were asked. Section C concludes with questions about appropriate style elements in order to visualise explanations of recommendation as well as different amounts of explanations for each recommendation in

the fixed internet. Section D offered 12 different design examples for transparent mobile event recommendation. The designs differ in the style element (e.g. text, icons, video, audio, text + icons) and the amount of explanations for each recommendation (e.g. 1, 3 or 5). At the end of section D, the participants were asked what style element is appropriate for a specific mobile event recommendation system.

H1) Recommender systems are used and helpful in the users' daily life

H1 implies that users understand the usefulness of recommender systems. They know that recommender systems help to get the information they are looking for by spending less time than searching by themselves.

The participants were asked whether they had used recommender systems for searching information that they were interested in. While 96.86% (308) did 3.14% (10) did not use recommender systems.

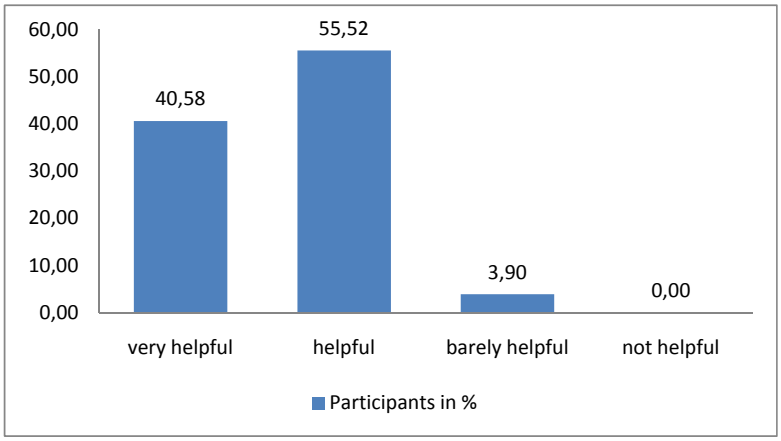

Figure 5 Usefulness of recommender systems

No user who applied recommender systems in the past said that these systems are not helpful. 96.10% said that recommender systems are very helpful or helpful in their daily life. Only 3.90% said that these systems are barely helpful.

H2) The relevance of transparency is more important for those users who know that personal information are processed within recommendations.

By addressing the H2, the participants were asked about their general knowledge about recommendations.

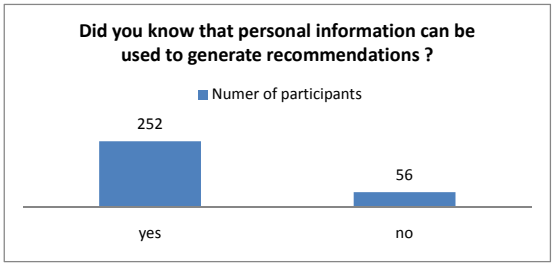

Figure 6 Awareness of processed personal information

252 participants (81.82%) know that getting personal recommendations often means that the system is accessing personal information such as user profiles or history data, while 56 participants (18.18%) did not know. The next question was only answered by the participants who are aware of this information processing.

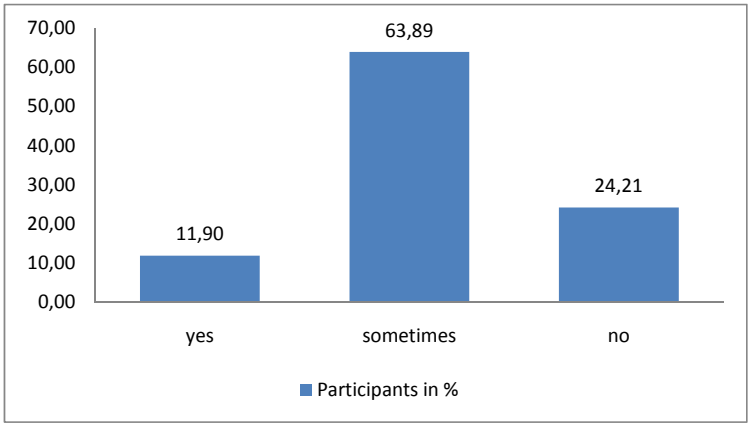

Figure 7 Understandability of recommendation

63.89% of the 252 users who knew that personal information was processed were only sometimes aware of the kind of information that was used (e.g. user profile data) to offer a recommendation, 24.21 % did not know.

Furthermore 308 participants who already used recommender systems were asked about the recommendations' understandability, visualisation and transparency on the fixed internet. 206 participants (66.88%) normally understand what items they get recommended. Only 79 participants (25.65%) said that they do not understand recommendations and do not know what they should do. When it comes to the visualisation of recommendations 197 participants (63.97%) said that today's visualisation is appropriate, while 111 users (36.04%) said today's visualisation is not sufficient to understand the nature of a recommendation.

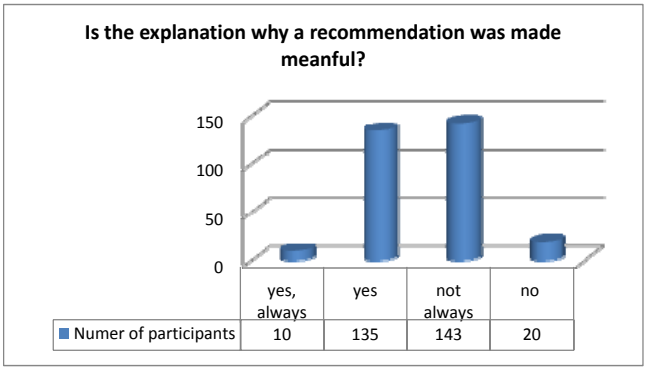

Figure 8 Transparency of recommendations

47.06% (145) of the participants said that the explanation of a recommendation is comprehensible in a way that allows understanding why a recommendation was made. Around 163 participants (52.92%) do not always or never know which personal information is processed to generate a recommendation and are not satisfied by the used visualisation.

H3) The combination of text and icons as a style element is the best solution to visualise transparent mobile event recommendations on a mobile device

In order to address H3 and the mobile environment, 12 different design examples for a transparent communicated mobile event recommendation are given as e.g. figure 12 demonstrates. These design examples differ in the style elements (e.g. text, icons, video, audio, text + icons) and the amount of explanations they provide for each recommendation (e.g. 1, 3 or 5). For each design example, the participants were asked whether they understood the recommended item, whether they understood why this recommendation was made (with reference to its explanations), whether the number of explanations were sufficient to understand the recommendation and finally, whether the given explanations were easy to follow.

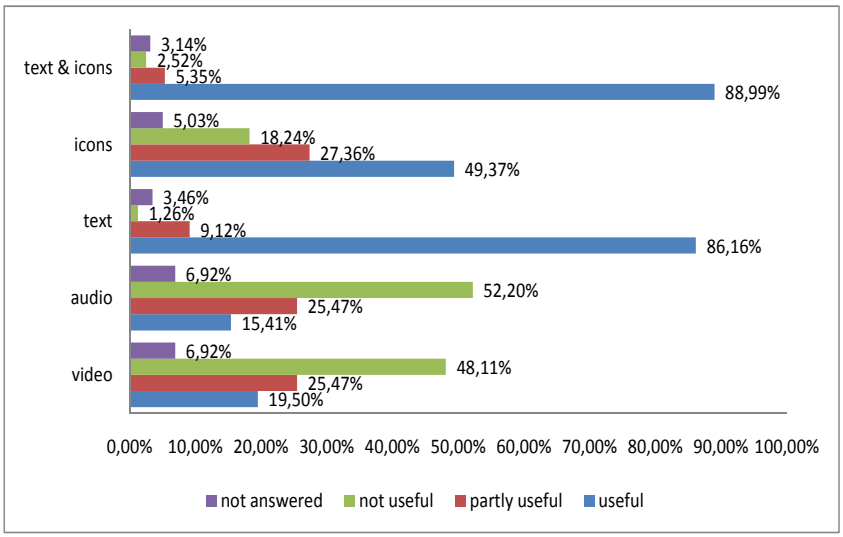

Figure 9 Preferred style element for transparent explanations on mobile devices

Later, the participants were asked which style element was appropriate to visualise a mobile event recommendation in a transparent way. 88.99% of all participants said that the combination of text and icons is the best solution to visualise explanations for recommendations. 86.16% said that text was a great way to describe an explanation. The usage of icons without any textual description was only an acceptable explanation style for 49.37% of the participants. Describing the nature of a recommendation by showing a video (19.50%) or playing an audio file (15.41%) were less accepted.

H4) Three explanations for one event recommendation are sufficient to offer transparency from users' perspective

As mentioned before, all design examples also differ in the amount of explanations for each recommendation. The participants were asked how many explanations are sufficient for a mobile event recommendation to offer transparency.

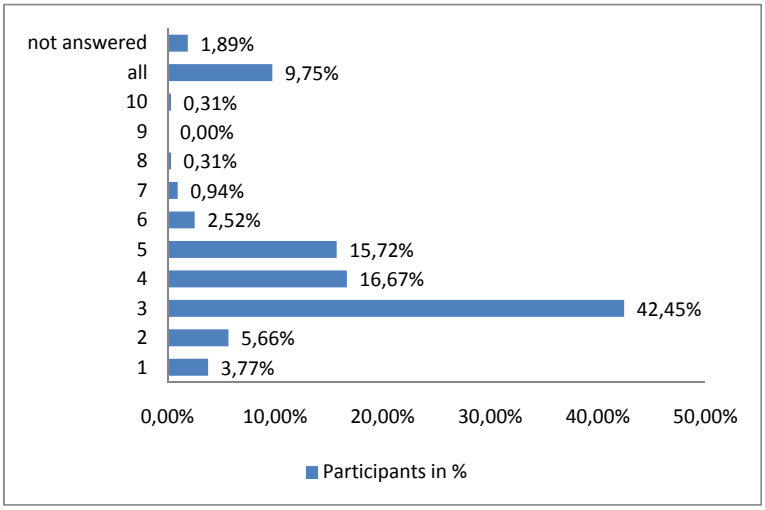

Figure 10 Number of explanations for each recommendation

42.45% of the participating users said that 3 explanations for one mobile event recommendation are sufficient to understand why a recommendation is made. If we use 1-5 explanations, 84.04% of all participants were satisfied.

All these results should indicate how mobile event recommendation can be visualised in a transparent way. Figure 9 shows one design example that combines text and icons in order to explain an event recommendation.

As mentioned in the beginning of section 4.3, the survey results support the conceptual design by offering insights into how to visualise an explanation for transparent recommendations on mobile devices. The relation between the survey results and the hypotheses are given below.

Nearly all participants who had used recommender systems said that these systems are helpful (96.10%) or at least barley helpful (3.90%) in their daily life (H1).

It was also indicated that 81.82% of all participants knew that recommender systems can process personal information in order to generate a recommendation. Furthermore, 81.10 % of the participants only knew in some cases or did not know what personal information was processed. In addition, 52.92% said that there was no sufficient explanation for a recommendation given that allows understanding what information was processed or why this recommendation was made (H2).

After presenting 12 different design examples for transparent mobile recommendations which differed in style elements as well as in the level of detail, 88.9 % of the participants pointed out that a description using “text and icons” might be the best way to visualise an explanation on mobile devices. The second highly preferred option was only “text” followed by “icons”, “video” and “audio” (H3).

The design examples also contained different levels of detail. 1, 3 or 5 different explanations for each style element were presented to the participants. Mostly 42.45% decided that 3 explanations for each recommendation are sufficient, followed by 4 (16.67%), 5(15.72%) and all (9.75%) (H4).

The limitations of these results are the following: The results are based on an explorative survey which is not representative. The survey only addresses mobile event recommendations

but the results may be transferable to mobile recommendations in general which have to be evaluated in future. Furthermore, the display size probably influences the amount of sufficient explanations for each recommendation.

Summing up, the results indicate what kind of style element might be useful to explain mobile recommendations in a transparent way. Based on these results, a prototype will be implemented. After that an evaluation in form of interviews will be conducted: one interview with users of the mobile event recommender system and another interview with experts (e.g. mobile service provider or mobile operator) who offer such a system.

4.4 User Matching

After the investigation of how transparency is defined and how to represent transparent mobile recommendations, it is also important to know what kind of information is relevant from the user's point of view. First, the information that can be used to be visualised is separated into available information and relevant information.

The available information is e.g. the service provider target group description which can include for instance age, gender, professionalism, occupation group, income, basic setting, interests, work attitude, personality, country, region, location, frequency of use or brand loyalty (Kotler and Bliemel, 2001). In addition there is user generated information as part of the available information as e.g. information that is stored in user profiles (Radmacher, 2007a). Such information can be a pseudonym, age, interest or other. Direct user feedback by for instance explicit answering of questions as "was the recommendation helpful?", indirect user feedback by deriving the user's behaviour through surf behaviour, mouse movements, scroll behaviour, retention period or iris movements (Fu, 2007) and information of a user as e.g. location information provided by a third party, completes the picture of the available information.

Relevant information is typically the kind of information the user pays most attention to. By looking into the already established research approaches (methodology) three different theories can help to answer this question. First the attention economy (Bleicher and Hickethier, 2002; G. Franck, 1998) which is based on the limited attention of a user. The high amount of available information cannot be searched by humans because their capacity is limited. Therefore it is important to offer the user a set of information that is probably interesting for him by filtering out irrelevant information. The transaction costs theory (Williamson, 1985) also provides relevant insights about the information relevance from a user's perspective. Looking for information takes time which produces costs. Finding relevant information is a less time consuming step and will reduce search costs. The third theory is about risk and uncertainty (Ripperger, 1998). Information that is provided for instance by a recommender engine has to be trustful. The user should have the possibility to check if the recommendation is right.

Trying to find a match between the service provider target group description and the user profile attributes involves a matching process which can be typically described by figure 11.

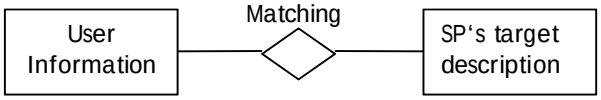

Figure 11 Matching

The classical matching can be done rule-based as given below:

IF

user_profile_attribute$_{i1}$(UPA$_{i1}$) = service_provider_attribute$_{j1}$ (SPA$_{j1}$)

AND/OR IF

user_profile_attribute$_{i2}$(UPA$_{i2}$) = service_provider_attribute$_{j2}$ (SPA$_{j2}$)

AND/OR IF

user_profile_attribute$_{in}$(UPA$_{in}$) = service_provider_attribute$_{jm}$ (SPA$_{jm}$)

THEN match

ELSE no match

Due to the fact that each user attribute has its specific relevance, each attribute needs to have a weight which expresses the relevance. A user profile (UP_i) consists of several user attributes (UPA). $UP_i = \{UPA_{i1}, \ldots UPA_{in}\}$. Each attribute has a name ($UPAN_i$) and a weight ($UPAW_i$) that indicates its importance to the user. $UPA_i = \{(UPAN_{i1}, UPAW_{i1}), \ldots , (UPAN_{in}, UPAW_{in})\}$. The main question that has to be answered by individual research is what factors have an impact on user's relevance in a specific application area. $UPAW_i = \{ A_i + B_i + C_i + D_i + E_i + \ldots. \}$

4.5 Integration of Transparency

The question of the integration of transparency requires us to investigate the structure of traditional recommender systems. The following structure of a recommender system is derived by literature research.

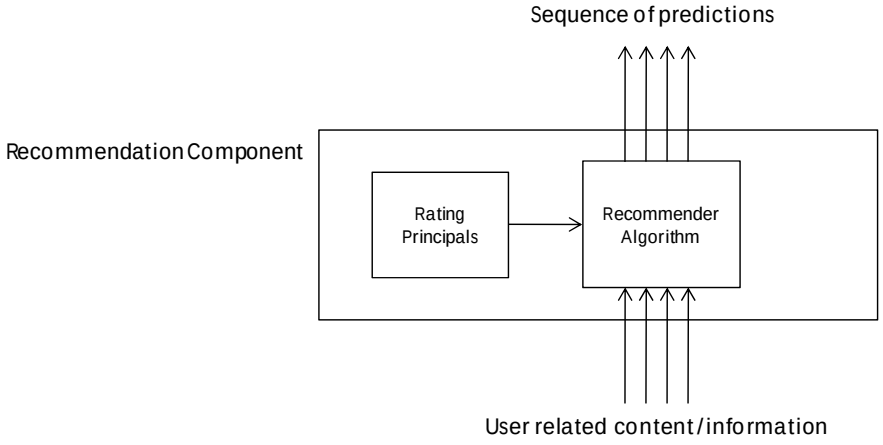

Figure 12: Components of classical recommender systems

A classical recommender system always consists of user related information as input, a recommendation algorithm, rating principals the algorithm is operating on and a sequence of predictions as output (Resnick and Sami, 2007). In order to offer transparency within recommendations, the following enhancements are proposed.

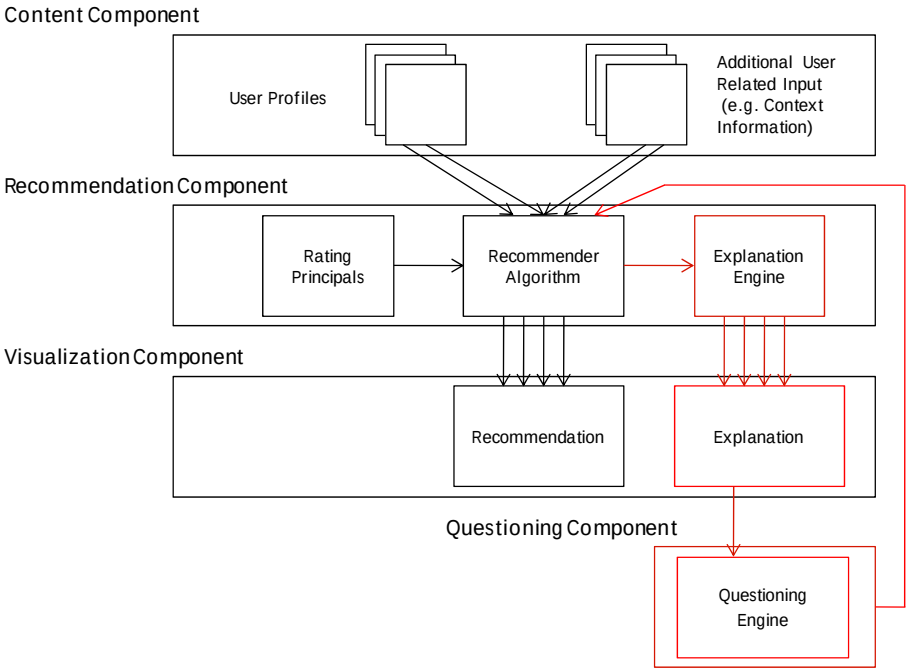

Figure 63 Transparency in classical recommender systems

The proposed architecture comprises three additional components: the explanation engine, the explanation and the questioning engine. The explanation engine is located within the recommendation component. After the recommender algorithm generated the recommendation, information about the system conclusion is transferred to the explanation engine which main task is the processing for the explanation. The component called explanation which is located in the visualisation component is responsible for the visualisation of the underlying conclusion. The visualisation can be performed by e.g. different style elements as mentioned at the end of section 4.3. The questioning engine allows to critique the system assumption for a particularly recommendation. Remember that transparency should help the user to understand why a particularly recommendation was made, especially in the case of a wrong recommendation. By offering transparency new direct user feedback is generated that can be used to refine existing recommendations.

To demonstrate the feasibility a prototype of a future real life application was developed that is operating on the previously findings. The application that is chosen is a transparent mobile event recommender system, called MoReCa.

Events are typically every kind of activity users can participate in, e.g. movies, concerts, lectures, meetings, dinners and others. An event is minimally described by its name, a location where it takes place and a time when it starts and ends. Why an event is recommended to a user can have several reasons. An event can be recommended based on user's interests, on the distance between the event's location and the user's current position, due to the fact that a couple of friends already accepted the recommendation or the user's calendar is just empty. The event, in this case the movie "Spiderman 4", is described by its name, the location, the date and the time. By asking the system why this recommendation is made, MoReCa will display explanations for the recommendation, given by figure 12.

Figure 74 Transparency in mobile event recommendations

An explanation, in this example, consists of an icon and textual description and enables the possibility to give explicit feedback in the form of yes the explanation is right, no it is wrong, it is inappropriate for this recommendation or by changing the order to express the relevance of an explanation.

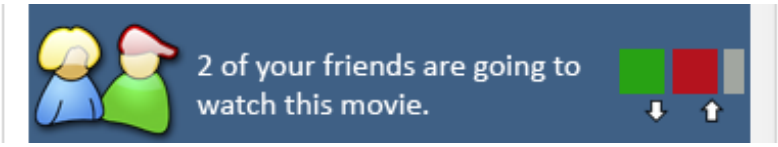

Figure 85 Transparent explanation of a mobile event recommendation

This representation of transparent recommendations can allow being more tolerant against wrong recommendations and providing active user feedback to refine recommendations.

Ongoing research brought us to interviews with experts from a mobile communication company with which Radmacher discussed the relevance of transparency regarding customer retention from an economic point of view. Without presenting the result in detail, Radmacher said that the current research results including the prototype are looking promising to every expert Radmacher asked and they are looking forward to seeing the application in action sometime. The experts believe that transparency within mobile recommendation will lead to a better understanding of mobile recommendations and will definitely increase the customer tolerance, acceptance and of course retention rate.

5 Requirements for legal compliance and legal safeguards for transparency in mobile marketing

Transparency is a central element of the European framework on data protection and privacy. Data subjects have the right to be informed about the identity of the controller, the purposes of the processing for which the data are intended and possible recipients at different stages of processing of the data as set forth in articles 10, 11 and 12 of the European Data Protection Directive (95/46/EC) and several other provisions on European and national level.

Transparency seemingly collides with the interests of at least some service providers as they tend to keep the details of their processes regarding personal data secret form the concerned data subjects. This might be due to a fear that otherwise customers might refrain from subscribing to the service but also for more reasonably justifiable reasons such as the protection of trade secrets from being explored by competitors.

The following sections will elaborate on legal issues relating to mobile marketing. In particular the transparency principle is examined in its legal grounds in the data protection legislation on European as well as on national levels in Germany and France. As most of the national legislation is based on European Directives, redundancy is inevitable to a certain extent. To avoid too much overlap, we chose to apply different use cases within the country reports. The legal evaluation shown will be transferable to most EC jurisdictions, however, due regard must be held to specialities in the national implementations of the European Directives. Finally the relation of transparency to interests of service providers such as the possible collusion with intellectual property rights is examined. In this course the current legislative process in Germany is described which attempts to strike a balance between the interest of credit rating agencies to protect their trade secrets and the necessary extension of the data subjects' rights of access.

5.1 Overview of relevant European provisions

The processing of personal data is regulated in a two EC directives,[5] both of which contain provisions regarding the processing of personal data for marketing purposes. The two privacy directives lay down definitions of parties involved in the processing of personal data, and contain regulations for the processing of different categories of data. They have been transposed into national law in the EU member states.[6]

Besides these the Unfair Commercial Practices Directive[7] contains provisions aiming at protecting European consumers against soliciting advertisement and marketing practices. The Unfair Commercial Practices Directive has been transposed into national law in the EU member states, too.[8] However, the regulations have not been included into the central legal

[5] 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. 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).

[6] See overview at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

[7] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

[8] See overview at http://ec.europa.eu/consumers/rights/index_en.htm.

regulation on Data protection but other specific laws such as the Act against Unfair Practices (Germany) or the regulations on Telecommunications (France).[9]

5.2 Involved parties

When analysing the obligations and rights of parties involved in mobile marketing it is necessary to assess which legal role the involved entities carry out. Directive 95/46/EC lays down the basic definitions of parties involved in the processing of personal data and presents the rights and obligations of these parties. For the sector of electronic communication Directive 2002/58/EC provides special rules for the processing of personal data.

'Personal data' shall mean any information relating to an identified or identifiable natural person (**'data subject'**); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 2 (a) Directive 95/46/EC).

In addition to the term data subject the Directive in Article 2 specifies further parties involved: data controller, processor, third parties and recipients:

'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. **'Processor'** shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. **'Third party'** shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data and finally, **'recipient'** shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

With regards to the processing of personal data in the electronic communication sector, further definitions in Article2 of Directive 2002/58/EC apply:

'User' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.

[9] The member states chose different approaches for the transposition and implementation of the directive. Some member states have disaggregated the "black list" enumerating unfair practices in the directive's annex and implemented it different pieces of their legislation. See: European Parliament Session Document A6-0514/2008 p. 9, online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0514+0+DOC+PDF+V0//EN

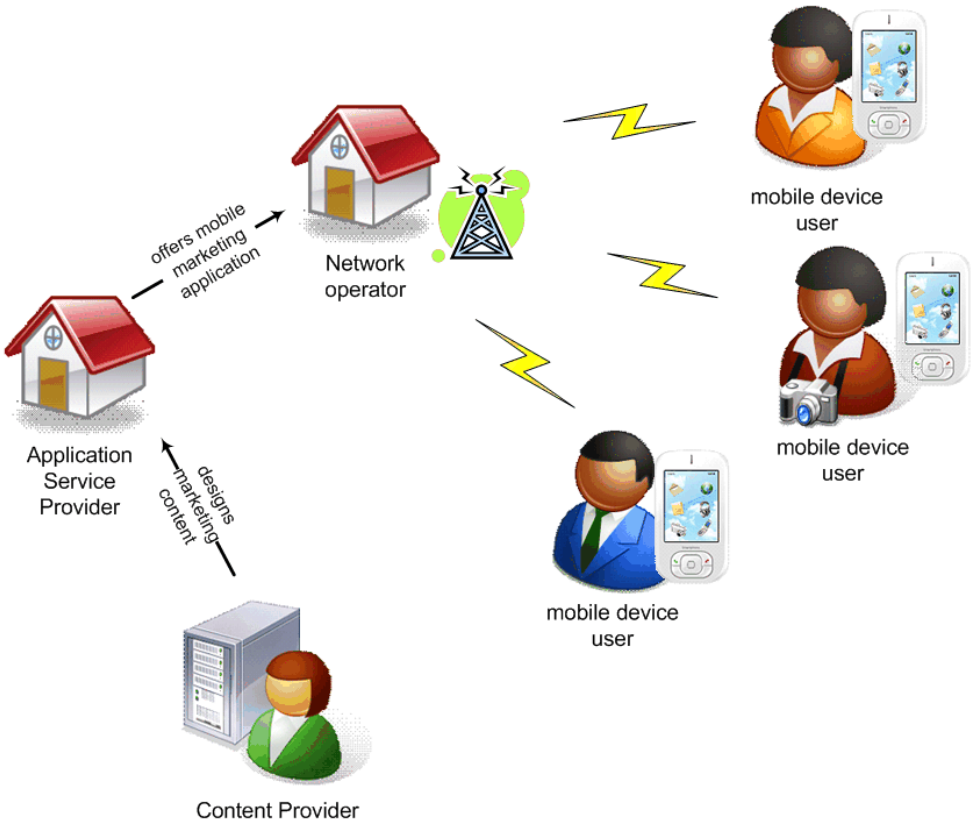

Figure 9: Parties involved in mobile marketing

The above figure presents parties involved in the provisioning of mobile marketing. The user or subscriber of the electronic service and device is the data subject to whom the personal data relates. The network operator is the data controller of traffic and location data relating to the data subject. The application service provider may act as a data processor for the network operator and data controller. Transmitting location or traffic data to the content provider is not necessary as he is only concerned with the design of the layout and design of the marketing message.

5.3 Categories of Data

The transmission of messages to a mobile device for marketing purposes usually involves different types of data, some of which are defined in Article 2 of Directive 2002/58/EC.

'Personal data' shall mean any information relating to an identified or identifiable natural person (see above 5.2). The criterion of personal data in respect to location based services has been further assessed within FIDIS already (Cuijpers, Roosendaal and Koops, 2007: p. 25).
'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

The legal requirements for lawful processing of traffic data are regulated in Article 6. Generally speaking, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication (Article 6 paragraph 1). Article 6 furthermore contains a specific section on the processing of traffic data for marketing purposes: according to Article 6 paragraph 3 traffic data may only be processed for the

purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. The Directive 2002/58/EC refers to the definition of consent given in Directive 95/46/EC, Art. 2 (f) of Directive 2002/58/EC. According to Article 2(h) of Directive 95/46/EC 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. Prior to obtaining the consent for marketing, the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of the processing (Article 6 paragraph 4 of D 2002/58/EC).

Location data which is necessary for the provisioning of the communication service is treated like traffic data (for example cell-ID that is needed to locate the mobile device and transmit a MMS to the mobile device). Location data that is necessary to provision a value added service[10] is not treated like traffic data.[11] Instead the below described provision of Article 9 of Directive 2002/58/EC applies.

In summary the following obligations and rights with regard to traffic data apply:

- erase or anonymise when no longer needed for transmission of a communication
- process for marketing purpose only based on subscriber's or user's consent,
- consent may withdrawn at any time,
- information prior to consent: type of traffic data and duration of processing,

'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

According to Article 9 paragraph 1 of Directive 2002/58/EC location data other than traffic data may only be processed when they are made anonymous, or with the consent of the users

---

[10] *Article 2(g) of Directive 2002/58/EC defines 'value added service' as any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof. Recital 18 further describes value added services as services for example consisting of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information. Mobile marketing messages can be considered value added services following this definition.*

[11] *See Recital 35 of Directive 2002/58/EC: In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent.*

or subscribers to the extent and for the duration necessary for the provision of a value added service. Even the informed consent of the subscriber cannot allow the provider to extent the duration beyond the time necessary to provide the service, however, a certain space for the interpretation of the purpose is given as different kind of services and levels of accuracy may require a longer retention of location data (see e.g. for the German law Wittern para. 13). 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.

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.

Processing of location data other than traffic data may only be carried out by persons acting under the authority of the network provider 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 summary the following obligations and rights with regard to location data apply:

- location data may only processed when made anonymous, or with consent of data subject,
- location data may only be processed to the extent and for the duration necessary for provision of the value added service,
- prior to obtaining consent, information must be given regarding the type of location data, the purpose and duration of processing, and a possible transmission of location data to a third party for the provisioning of the value added service,
- consent can be withdrawn at any time,
- the data subject must be able to temporarily refuse the processing of location data at any time.

A further category of data is relevant for the provisioning of mobile marketing is customer data. The two EC privacy directives do not contain special regulations regarding this category of data. According to the German Telemedia Act customer data comprises name, address, customer reference number, profile data (hobbies, taste, preferences). (See below 6.1.1).

5.4 Unfair Commercial Practices

The E-Privacy Directive 2002/58/EC contains regulations of unsolicited communications in Article 13. Paragraph 1 deals with direct marketing by means of email and fax. SMS and MMS are also covered by the directive, even though they are not directly mentioned in Article 13 of the E-Privacy Directive. According to Recital 40 of the E-Privacy Directive safeguards shall be provided for subscribers against intrusion of their privacy by unsolicited communications, including SMS messages.[12] In the scope of this Directive the term

[12] As for communications via Bluetooth see below chapter 7.2.1.

'electronic mail' further means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient (Article 2(h)). Paragraph 1 once more clarifies under the perspective of unsolicited communications that the use of electronic mail for the purposes of direct marketing is only allowed in respect of subscribers who have given their prior consent.

If a company obtains electronic contact details of its customers such as the user's email address in the context of the sale of a product or a service, the same company (!) may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

Furthermore, member states are called upon to introduce legislation ensuring that unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications (Article 13 paragraph 3).

In summary the following obligations and rights with regard to unsolicited communications apply:

- direct marketing via electronic mail permissible by company for similar service, product (here: no consent needed, but opt-out)
- upon collection of electronic contact details and on the occasion of each message: give opportunity to object use of data for marketing purpose

The Unfair Commercial Practices Directive further specifies misleading commercial practices in section 1 and aggressive commercial practices in section 2.

6 Country report Germany

6.1 Lawfulness of mobile marketing

When considering the lawfulness of mobile and location based marketing a variety of legal aspects need to be taken into account. As the answers to questions regarding the collection and processing of personal data are coherent with those arising with the application of LBS for other purposes than marketing we like to refer to the substantial evaluation of the related legal questions in German law previously provided within FIDIS (Cuijpers, Rosendaal, Koops, 2007: 79-93). This chapter concentrates on issues specific to mobile marketing in general and mobile recommendation systems in particular. However, as far as necessary for completeness or for better comprehension, the provisions described earlier will be readdressed below. The analysis will comprise in particular the German Data Protection Act (Bundesdatenschutzgesetz, BDSG), the German Telecommunication Act (Telekommunikationsgesetz, TKG) and German Law on Telemedia (Telmediengesetz, TMG). Some specific regulations not related to privacy in regard to the advertisement's content may also directly or indirectly affect the legal availability of certain channels for mobile marketing. We will exemplarily cover a selection of such special issues in 6.1.4 below.

The German Legal regime will be exemplified based on the following use case. Advertisements are sent via SMS or MMS to persons located within a certain area and that belong to a target group that had indicated interest in the specific offers to the content provider. The network operator necessarily needs the current location data to provide the mobile phone service and mandatorily collects them as a result of the Data Retention Directive. An application service provider maintains a database of persons interested in certain commercial information. The customers have previously signed in for the service, willing to receive information they are interested in, e.g. a travelling salesmen is interested in restaurants when being in a foreign town during lunchtime. The content provider delivers the actual content of the advertising messages to be sent. In a more advanced state the recommender system could collect further information on interests of the user and his social relations to match with interests of friends. Then the legal regulations named below evidentially will apply for all participants that subscribe to the system.

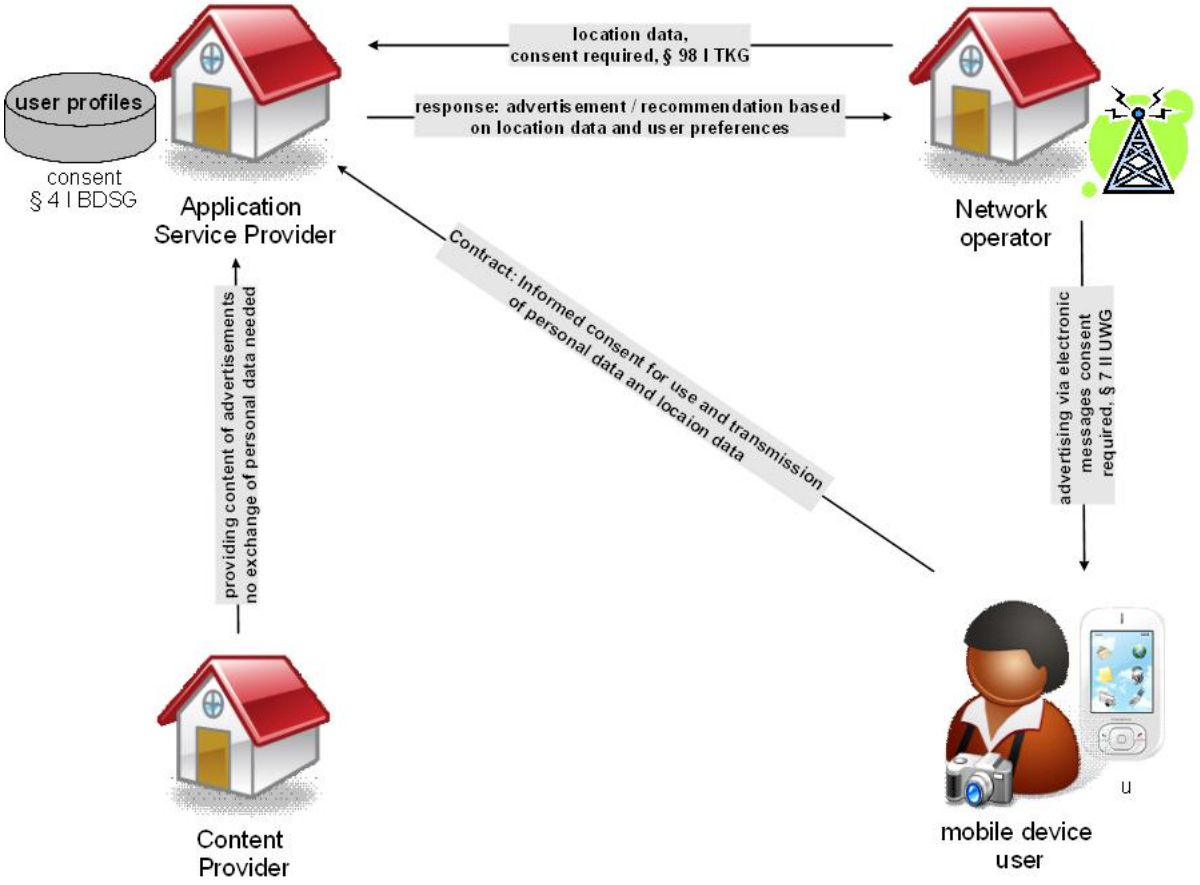

Figure 10 Data flow and consent requirements

In addition to this setup the introduction of trusted intermediates may increase the level of privacy for the user. Such a system has been elaborated by the EC-funded project PRIME.[13] The intermediary will reside between the network operator and the application service provider anonymising the respective data flows. The methods set forth there may be applied for mobile marketing as well, however, they will not be part of the considerations here.

6.1.1 Legal basis or consent?

In regard to the regulations on data protection and privacy every processing of personal data must be justified by specialised laws, a regulation within the BDSG or informed consent of the data subject, § 4 sec. 1 BDSG. As the TKG and TMG regulate most of the issues arising in connection with LBS these and subsidiary the regulations of the BDSG will be the focus of the following analysis.

For telecommunication service providers specific rules for the use of **customers data** exist in § 95 TKG. Telecommunication service providers may use customer data to advertise towards customers they have a contractual relationship with unless the customer objected to this use,

[13] The LBS services developed within the PRIME project feature a apothecary finder, where the customer individually triggers the service and a pollen warning where an allergic person may order to be continuously informed about the pollen concentration at the his location. The social, legal and economic requirements for these prototypes are set forth in Schumacher 2008; an evaluation of the prototype and the implementation of the requirements are given in Bramhall 2008.

§ 95 sec. 2 s. 2 TKG. Other telecommunication providers, not having a contractual relation with the data subject, need the consent of the subject before addressing him, § 95 sec. 2 s. 1 TKG. It is furthermore not permissible that the service is only provided under the condition that the customer declares his consent for the use of his data beyond the extent necessary to render the services, § 95 sec. 5 TKG.

The collection and processing of **location data** by the telecommunications service provider is regulated in §§ 96 and 98 TKG. As far as the processing is required to provide the service, for billing purposes or to comply with legal requirements this is allowed by the law, §§ 96 sec. 2, 97 TKG. The transmission to the application service provider constitutes a change in purpose and thus requires a separate justification. Such a transmission is permissible by law for anonymous location data or with consent of the data subject, § 98 sec. 1 TKG. Thereby it is sufficient to obtain the consent once within a master agreement.[14] As at present identification of the user occurs via the access device used (mobile phone, pda) problems may arise as the device may easily be passed on undetected by the provider to third persons.[15] For this reason the law provides that the person that consented has to inform other users of the device of the activated tracking functionality. The user further has the right to withdraw his consent at any time and it must be possible to oppress the transmission of location data temporarily.

As for the processing of customer and location data by the application service provider § 15 sec. 1 TMG allows to collect and process the data necessary to provide the service. To deliver the localised SMS the application service provider needs information on the current location of the customer and some identification to match the location with the given interest profile of the user. Processing beyond this extent requires the user's consent.

For recommender systems informed consent of the data subject is a mandatory requirement to use or transmit location data, § 98 sec. 1 TKG. In case location data will be transmitted to third parties, e.g. friends, the informed consent must cover this transfer of information as well.

6.1.2 Consent for marketing towards natural persons

While the TKG and TMG regulate whether processing of customer and location data is legal the German Act against Unfair Practices (Gesetz gegen Unlauteren Wettbewerb, UWG) decides whether taking up the contact as such is allowed for advertising purposes. Marketing by means of automated calling systems, facsimile machines or electronic mail requires the consent of the consumer, § 7 sec. 2 s. 2 UWG.[16] SMS and MMS are considered to be electronic messages in the sense of the UWG.[17] Also other existing technologies such as Bluetooth and forthcoming inventions require the consent of the user. In Germany the transformation of article 13 of Directive 2002/58/EC was defined as a specific example of the generally forbidden unreasonable annoyances, § 7 sec. 1 UWG. Thus other similar or even more annoying measures for advertising are forbidden as well. This encompasses in particular all means of advertisement deploying equipment of the user, by consuming bandwidth, memory and where effective countermeasures to filter the unwanted content are not available. However, there is no case law on the revised version of the UWG yet.

---

[14] See reasons given by the German Government, Bundestagsdrucksache 15/2316, p. 89, online: http://dip21.bundestag.de/dip21/btd/15/023/1502316.pdf.
[15] See detailed problem statement in Cuijpers, Rosendaal, Koops, 2007: 92.
[16] § 7 sec.2 is the German enactment of Article 13 of the E-Privacy Directive 2002/59/EC.
[17] See recital 40 of the E-Privacy Directive 2002/58/EC. For further references see Piper, Ohly 2006: § 7 UWG, para. 66.

Requirement for opt-in

The necessary consent of the consumer must be conducted without force (free), needs to specify the purposes (specific) and the identity of the data processor (informed). When it is contained within general terms and conditions it is necessary that the consumer acts to positively declare his agreement for example by signing a separate declaration or by marking a checkbox (**opt-in**). As recently decided by the Bundesgerichtshof it is not sufficient when terms and conditions contain a consent clause and leave it open to the consumer to cross the relevant section out.[18] Such an opt-out is only permissible for marketing using conventional "snail" mail.[19] In the case decided by the court the vendor of a loyalty program used a written contract with lengthy terms and conditions. It was left to the customers, whether they provide information on their mobile telephone number and their e-mail address to receive extra benefits and announcements regarding their achievements within the loyalty program. The relevant provision was placed at the end of the contract, specifying that the user confirms his consent that his data will be used for marketing and market analysis by conventional mail and if requested via e-mail and SMS. To opt out the customer had to mark a checkbox. The court ruled that this violated the legal requirements for a valid opt-in.

Exception of the opt-in requirement

The strict requirement for an opt-in does not apply, when the following four cumulative conditions are met, § 7 sec. 3 UWG:

- the customer's e-mail address has been received by the company in the course of the sale of good or providing of services,
- the address is used for direct marketing by the company for similar goods or services
- the customer did not object and
- the customer receives clear and unambiguous information about his right to object further processing during the collection of the data and with every use of the data. Filing the objection must not cause any costs besides the usual costs for the transaction.

This important exception allows marketing towards existing customers. But as this exception allows only marketing for similar goods and services of the company that collected the data (point 2 above) is consequently not allowed to advertise for other entities or to combine own advertisements with messages for such entities including those of the same group of companies (Hefermehl, Köhler, Bornkamm, 2008: § 7 UWG para. 89). The question has been raised as to how far the condition "similar" may be stressed. This interpretation needs to be done in conformity with the EC Directive 2002/58/EC, as the origin of § 7 sec. 3 UWG (Spindler, Schuster, § 7 UWG para. 57). At least goods or services that are interchangeable in the sense that they may meet the same demand fall under the exception. Marketing for accessories of the goods bought by the consumer already are also covered, e.g. hooks and bait when a hinge was bought (Hefermehl, Köhler, Bornkamm, 2008: § 7 UWG para. 89).

[18] See judgement of the Bundesgerichtshof 16. Juli 2008, VIII ZR 348/06, I. 3. a).

[19] However, it is debated to introduce opt-in as a general requirement for advertising into the BDSG. The draft bill on the so called permission marketing is under current debate in the legislative process. While welcomed by Data Protection Commissioners it is combated by the marketing industry. A decision is not awaited until the deadline for this report.

Finally it shall be mentioned that the burden of proof for the lawfulness resides with the company (Piper, Ohly 2006: § 7 UWG para. 71). So even if a written form is not explicitly required for the consent to be valid it is very advisable to have a revision proof evidence that the consumer has in fact consented.

Due to its limitation to existing customers the named exception may replace the consumer's consent in but a small fraction of the possible targets of the use case for recommender systems. Even if § 7 sec 3 UWG allows to address the consumer consent is still needed for the use of the location data even it the telecommunication service provider itself intends to advertise for products similar to those already sold.

6.1.3 Consent for marketing towards companies

German law does not differentiate in § 7 UWG between consumers and companies as it intends the protection of all market participants including competitors, other businesses and consumers. Thus the same regulations apply in this field and a specific, informed consent is required. Prior to the transformation of Directive 2002/58/EC into German law it had been possible to revert to a presumed consent with other companies. This easement has been discarded with the reform (Piper, Ohly 2006: § 7 UWG para. 64).

6.1.4 Lawfulness in regard to the content of mobile marketing

The content of a message sent within mobile marketing is legally relevant for the mandatory content regarding information and the possibility to object to further messages on the one hand and possibly problematic content of the marketing message itself.

Mandatory content

Within every message the consumer must be informed in a good visible manner about his right to object to any further messages, § 95 sec. 2. s. 3 TKG.[20] Advertisements that enable a consumer to conclude a contract must also provide some minimum information, § 5a UWG.[21] These comprise namely:

- the main characteristics of the product, to an extent appropriate
- the geographical address and the identity of the trader
- the price inclusive of taxes, or the manner in which the price is calculated, and additional freight, delivery or postal charges
- conditions for payment, delivery, performance and the complaint handling policy
- due information on the right of withdrawal or cancellation

The existing limitations of SMS and MMS in respect to the size of the message may cause problems for recommendation systems as all the mandatory information must be delivered with the advertisement, once the duty to inform the user is triggered. This is the case once the advertisement enables the consumer to conclude a contract, which does not mean that a binding contract is necessary. To trigger the duty for due information it is sufficient that the essential contents of the contract are transmitted, e.g. the goods or services concerned and the price (Hefermehl, Köhler Bornkamm 2009: § 5a UWG para. 29). This is not the case for

[20] If circumstances allowed application of the exception to the opt-in requirement, § 7 sec. 3 nr. 4 UWG would demand the same information about the right to object as well.
[21] § 5a UWG is based on article 7 sec. 4 of the Unfair Commercial Practices Directive 2005/29/EC.

image marketing or plain reminders. Other communications, in particular offering services that are intended for mobile use (maps, ordering tickets etc.), will require that the necessary information must be included in a means appropriate for the used communications medium.

Legally problematic Content

For mobile marketing in general and advertising on the basis of location based services the content and the kind advertised product may have in special cases a major impact on the lawfulness of the strategy. Rules that regulate advertisements for certain products and services (e.g. dangerous chemicals, drugs) or by certain professions (e.g. physicians, advocates) usually do not differ between the media used and the location. However, for some goods special restrictions may apply that effect in particular use cases of mobile recommendation systems. For the sake of completeness some of these provisions are named below.

Advertising gambling is permissible only for publicly accredited organisers (lotteries, casinos). Advertisement for such services is not allowed on TV, internet or other means of telecommunication. In case this limitation leaves any room for recommendation systems the advertisement may neither directly address minors nor encourage or stimulate the addressee to engage in the advertised game.[22] As the advertisement shall not directly stimulate to engage in gambling, advertising on a basis of location based services for gaming possibilities, e.g. the casino which is located "just around the corner", may be permissible only in special situations. This will probably exclude any advertising at a very close distance to the casino or during its opening hours. Furthermore the prohibition to address minors could make it necessary to know and to verify the addressees age. This raises further questions in regard to privacy but also how the age can technically be verified in cases where only a device is known but not who the current holder is. As particular contracts for mobile telephony are regularly concluded by the parents who then pass on phone and SIM to minors, it is difficult to rely only on the contractual customer data.

Advertising towards minors in telemedia is restricted in the Jugendmedienschutz-Staatsvertrag (JMStV).[23] Contents that glorify war or violence are cruel or racialist are completely inadmissible, otherwise pornographic or indexed content may require the provider to verify the consumer's age prior to advertising for such goods, § 4 JMStV. Advertising for content restricted to adults is limited as to its contend and make and it must not directly appeal to minors, § 6 JMStV. An identical regulation is contained in the appendix to § 3 UWG Nr. 28, which forbids to target children with advertisements. When advertising for alcohol in any media or tobacco in telemedia it is not allowed to explicitly target minors nor may it display minors consuming alcohol or tobacco.

Other specific restrictions may be contained in the following non-exhaustive list of provisions on marketing:

- Pharmaceuticals with a prescription requirement may not be advertised except to medical staff, § 10 HWG.[24]

[22] The federal stats are the competent body to regulate gambling and lotteries. The states concluded a contract to unify regulations on gambling. The regulation on advertisements may be found in § 5 Glücksspielstaatsvertrag 2007,online:
http://www.hessenrecht.hessen.de/gesetze/Staatsvertraege/90-GlueckspielStV/GlueckspielStV.htm
[23] Jugendmedienschutz-Staatsvertrag, online: http://hh.juris.de/hh/gesamt/JMedienSchStVtrG_HA.htm
[24] Heilmittelwerbegesetz, online: http://www.gesetze-im-internet.de/bundesrecht/heilmwerbg/gesamt.pdf

- Advertising dangerous chemicals requires adequate indication of the hazard, § 15a ChemG.[25] Adequate displaying the hazard warning may be difficult to ensure on an unknown device.
- Professional codes of conduct for physicians,[26] lawyers,[27] tax consultants,[28] and several other professions
- Restrictions had been planed in schools or close to schools as well as in buildings of government agencies. Respective regulations may be taken by local administrations already.

6.2 Conclusion

For recommender systems and other location based techniques of marketing the consent of the user is a mandatory requirement under German law. Due to the interlocking and dual applicability of the regulations on telecommunication (processing of location data) and regulations against unfair competition (using telemedia as a means of communication) there is not much room for a lawful constellation of marketing that does not depend on the explicit users consent. Even if a company of the network operator itself would offer the service and thus no transmission of location data to a third party would be necessary, the utilisation for advertisement in favour of a third party constitutes a change of purpose which is not covered by the law.

As the German legislator voted for an opt-in for such kind of marketing application service provides should ensure that the declaration of consent is clear and unambiguous and, when declared together with other declarations of will, should preferably be composed as a separated declaration. When contained within general terms and conditions it is necessary that the customer positively acts to indicate his approval, e.g. by marking a checkbox.

In an overall view transparency is a central requirement for mobile marketing and mobile recommender systems in Germany. The need for an informed consent ensures that the user knows beforehand about the processing and transmission of location data. As consent is also required to process the user's interest profile by the application service provider transparency is ensured in the relationship to that party as well. Based on European principles of consumer protection the advertisements need to be transparent in respect to their content as well, however, the latter does not concern transparency in the sense of data processing.

[25] Chemikaliengesetz, online http://bundesrecht.juris.de/bundesrecht/chemg/gesamt.pdf
[26] cf. § 28 Musterberufsordnung Ärzte, online: http://www.bundesaerztekammer.de/page.asp?his=1.100.1143.
[27] § 43b Bundesrechtsanwaltsordnung (BRAO), online: http://bundesrecht.juris.de/bundesrecht/brao/gesamt.pdf.
[28] §§ 10 - 21 Berufsordnung der Bundes-Steuerberaterkammer (BOStB), online: http://www.steuerlex.de/ficht/BOStB.htm.

7 Country report France

Direct marketing refers to any technique of personalised marketing-communication, using processing or databases of personal data with the purpose of establishing an interactive and measurable dialogue with an identified target.[29] Mobile marketing consists of using mobile phones to reach the target. It could makes use either of the additional information made available thanks to the use of a mobile device related to the location of the individual (the so-called 'location-based services') or of the new possibilities of communicating with the user via a mobile device (e.g. SMS/MMS, Mobile Internet, Bluetooth networks).

Mobile marketing is a promising market in France. Its development has been first hindered by the control of the three main mobile operators over the unique mobile platform, Gallery. Even though this platform has permitted to structure mobile content and their diffusion, the restrictive advertisement policy has first put a limit on the development of mobile marketing. Mobile advertising was technically controlled by mobile operators. It followed that in 2006, 90% of the income from mobile marketing was generated by mobile operators.[30]

The development of new mobile search engines and of new access means to mobile Internet, such as 2D barcode or Bluetooth, has however forced mobile operators to open their advertising policy on Gallery. Mobile operators have moreover announced that they were open to share their databases with all search engines.[31]

The growth of mobile marketing has required the definition of a clear legal framework to protect users from abusive marketing practices. The European legal framework has been transposed in France in 2004 via the LCEN[32] (*loi pour la confiance dans l'économie numérique* – Law for Trust in Digital Economy). To that effect, an opt-in system has been introduced for direct marketing with commercial content and based on the contact details of natural persons Other forms of marketing such as direct marketing to legal persons or without a commercial content should however comply with the more general rules set up by the Data Protection Act.

7.1 Transposition of the European framework on direct marketing into French legislation: Overview.

Article 13 of the E-Privacy Directive has been transposed in France by article 22 of the LCEN. This article modifies the French Consumer Code and the Posts and Electronic Communications Code (hereafter referred to as 'CP&CE') to adjust the French legal regime on direct marketing to the European legal framework. The core of the regulation is however contained in Article L.34-5 CP&CE. The Consumer Code only provides for the full application of the provisions of such article to any sale of goods or any provision of a service that takes place without the simultaneous physical presence of the parties between a consumer

[29] FEVAD, Code de déontologie des professionnels du marketing direct vis-à-vis de la protection des données à caractère personnel, 2003, available online at (in French) : http://www.cnil.fr/index.php?id=2474
[30] LeJournalduNet, *Enquête publicité sur mobile : un marché encore balbutiant*, 27 March 2007, available online at : http://www.journaldunet.com/diaporama/070327-mobile-enquete-pub-mobile/1.shtml
[31] Ibid.
[32] Loi pour la confiance dans l'économie numérique, n°2004-575 of 21 June 2004. The Act transposes the E-Commerce (Directive 2000/31/EC) and the E-privacy Directive (Directive 2002/58/EC).

and a professional who, in concluding that contract, use one or more distance communication systems to the exclusion of any other means (Article.L.121-20-5).

Article L.34-5 CP&CE prohibits direct marketing, via an automatic calling machine, a facsimile machine or an electronic mail system, using the contact details of a natural person who has not consented to being canvassed by such means.[33]

Direct marketing is further defined as 'the sending of any message intended to directly or indirectly promote goods, services or the image of a person selling goods or providing services'. Direct marketing will thus include all messages with a commercial nature for marketing and directed to natural persons irrespective of the communications means used: automatic calling machine, a facsimile machine or an electronic mail system.[34] It follows that direct marketing to legal persons and communications whose content does not qualify as 'commercial' are excluded from the scope of the article.

Article L.34.5 CP&CE introduces an opt-in system. It explicitly prohibits direct marketing without the prior consent of the recipient of the message. Derogations are foreseen for direct marketing by electronic mail provided that three cumulative conditions are complied with: a) the contact details were directly obtained from the recipient; b) the information relates to similar products or services provided by the same natural person or legal entity; c) the recipient is expressly and unambiguously given an opportunity, via a simple means and at no cost to himself other than the cost of transmitting a refusal, to oppose the use of his details when they are collected and each time that an electronic mail is sent to him for marketing purposes. The sending of direct marketing without the prior consent of the user is punished with a fine of 750 euro per email unlawfully sent (article R.10-1 CP&CE).

The right to object is pivotal to the system: the sending of direct marketing messages via an automatic calling machine, a facsimile machine or an electronic mail system should provide the recipient with a valid means through which he may effectively request that such communications cease, at no cost other than that of transmitting the said request. In 2003, a specific procedure was implemented in order to facilitate the exercise of the right to object. The user receiving unsolicited SMS could send a SMS with the text 'STOP' to the sender. The sender subsequently had to stop sending commercial SMS to the user, to inform him that his request had been taken into account and to delete the personal data from his processing. In case the sender did not comply with this obligation, the sender could report this infringement to their mobile operator's hotlines.

Despite this system, consumer organisations have denounced the significant increased of spam on mobile phones and the correlative number of senders that did not comply with consumers' requests. A specific platform dedicated to the fight against mobile spam has thus been implemented by the government and mobile operators. The platform is operative since the 15th November 2008. More than 10.000 reportings had been received in the first two weeks after the launch of the platform. The platform is accessible via a short number, 33700. Mobile phones users can forward the spam to this number. They will then be asked to enter

---

[33] The French text uses the term « *prospection* » that is literally translated in English as « canvassing ». However, for the purpose of this deliverable the term "marketing" will be preferred insofar, in this context, the term seems more adequate.

[34] CAPRIOLI E.A., *Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel*, Etude n°7, Communication Commerce électronique n° 2, February 2005.

the phone number of the spam sender. The platform will enable to inventory the messages received and the spam sender's numbers, to identify them, to block the spam received by users and to further prosecute the spammers whenever possible. This operation costs to the user the price of 2 SMS (1 for the copy of spam and one to communicate the number of the spammer).

Finally, it is worth mentioning that the CNIL, the French data Protection Authority, is given the authority to deal with complaints related to direct marketing which makes use of a natural person's contact details. Additional information on the doctrine developed by the CNIL on the processing of personal data for marketing purposes can be found in two Codes of Conduct which have received its prior approval: the Code of Conduct on Electronic Direct Marketing from the SNCD (*Syndicat National de la Communication Directe*) and the Charter on Emailing from the UFMD (*Union Française du Marketing Direct*).[35] The later Charter defines deontological rules on the collection and use of electronic contact details with purposes of direct marketing.

7.2 Mobile marketing towards natural persons for commercial purposes

Article L.34-5 CP&CE prohibits direct marketing, via an automatic calling machine, a facsimile machine or an electronic mail system, *using the contact details of a natural person* who has not consented to being canvassed by such means. This narrow definition raised the question of whether mobile marketing via SMS, MMS and Bluetooth marketing were falling under the scope of application of this article.

In line with Recital 40 of the E-privacy Directive, the CNIL has been prompted to acknowledge SMS and MMS to emails. Mobile marketing through SMS and MMS thus falls under the scope of application of the more restrictive provisions of Article L.34-5 CP&CE. This solution was not so obvious with regard to Bluetooth marketing but the CNIL, contrary to other European countries such as the UK, has also included this new type of marketing into the scope of application of article L.34-5 CP&CE.

Before entering into the analysis of the provisions of article L.34-5 CP&CE, it appears necessary to define its scope of application, in particular in relation to Bluetooth marketing. Additional considerations relative to the processing of location data for marketing purposes will be referred to at the end of this section.

7.2.1 Scope of application: the difficult problem of Bluetooth marketing

SMS, MMS and "blue marketing" as emails

The wording of the article L.34-5 CP&CE only refers to direct marketing via automatic calling machine, fax or an electronic mail system. Neither SMS, MMS nor messages sent via Bluetooth could be fitted in the first two categories. It thus appears necessary to examine whether they meet the elements contained in the definition of electronic mail systems.

Article 1 LCEN transposes the exact wording of the definition of email contained in article 2(h) of the E-Privacy Directive. « Electronic mail » is defined as any text, voice, sound or image message sent over a public communications network, which can be stored on the

[35] Both Codes of Conducts are available (in French) online on the website of the CNIL at : http://www.cnil.fr/index.php?id=2474

network or in the recipient's terminal equipment until it is collected by the recipient'. It follows that in order a message to qualify as email, three cumulative conditions should be met:

a) The message should consist in a text, voice, sound or image,

b) The message should be sent over a public telecommunication network and

c) The message should be stored either on the network or in the recipient's terminal equipment until it is collected by the recipient

It is obvious that SMS and MMS are text, voice, sound or image messages sent over a public telecommunication network and can be stored either on the network or in the recipient's equipment until it is collected by the recipient. Mobile marketing making use of SMS and MMS will thus fall under the provisions of article L.34-5 CP&CE. This interpretation, followed by the CNIL, echoes Recital 40 of E-Privacy Directive and is expected to prevent to overloading users' electronic communications networks and terminal equipments.

The solution is however not that obvious for Bluetooth marketing. As discussed by KOSTA *et al.*,[36] it is not always clear, from European legislation, whether commercial communication sent over Bluetooth networks could actually be acknowledged as emails. The CNIL has however considered that, under French law, Bluetooth marketing was falling under the definition of emails.[37] The CNIL did not detail the reasons for this interpretation. It thus appears necessary to analyse whether the transposition of the telecom Package into French Law allows such interpretation.

a) It is not under debate that marketing information sent via Bluetooth is a "text, voice, sound or image message",

b) It should thus be checked whether the ad hoc communication network originated by a Bluetooth communication could qualify as 'public communication networks".

Article L.32§3 CP&CE defines 'public communication networks' as an electronic communication network established or used for the provision of electronic communication services to the public or of public communication services by electronic means. Any communication network that fulfills one of these two functionalities will thus qualify as public.

Electronic communication services (article L.32 §6 CP&CE) consist in providing wholly partly electronic communications (excluding services of edition or distribution of public communication services by electronic means). Bluetooth marketing does not consist in the provision of electronic communications and thus does not fall under the concept of 'electronic communication services to the public'.

'Public communication services by electronic means' are defined (article 1 LCEN) as services that "put at disposal of the public or categories of public, by electronic means, signs, signals, text, images, sounds or message of all nature that do not qualify as private correspondence." Bluetooth marketing undoubtedly consists in putting a message at the

[36] KOSTA E., VALCKE P. & STEVENS D., '*Spam, spam, spam, spam… Lovely spam!' Why is Bluespam different?*', International Review of Law, Computers and Technology, Manuscript accepted in July 2008, *In press*

[37] CNIL, *Pas de publicité via Bluetooth sans consentement préalable*, 13 November 2008, available online at : http://www.cnil.fr/index.php?id=2549&tx_ttnews[tt_news]=1&tx_ttnews[backPid]=17&cHash=b983e4e78e

disposal of the public (anyone passing by the hotspot and accepting the communication can receive the message) by electronic means. Furthermore, Bluetooth marketing is clearly a public communication. With regard to this last requirement, it is worth stressing that the qualification of Bluetooth marketing as email is not incompatible with the fact that it consists in a public communication. The French Constitutional Court[38] has soon stated that emails were not *per se* 'private communications' but that their qualification in private or public communications would depend on the content of the message and the context. In that sense, whenever a service intends to diffuse emails with a content that cannot qualify as 'personal' to undefined persons, these e-mails will fall under the rules of public communication and will not be protected by the secrecy of communications.[39] Emails thus do not always fall under the protection of the secrecy of communications and can perfectly have a public nature under French law.

It thus seems likely that Bluetooth marketing would be deemed to use a public communication networks.

c) Finally, the definition of emails requires that the message can be stored on the network or in the recipient's terminal equipment until it is collected by the recipient. Bluetooth requires a simultaneous communication and does not allow the message to be stored on the network but the message can be stored in the recipient's terminal equipment until it is collected (opened) by the recipient. As recall ASSCHER and HOOGCARSPEL "anything can in principle be stored on terminal equipment, provided it has the appropriate functionality".

It follows that it is likely that commercial communications sent over Bluetooth networks could be acknowledged to emails for the purpose of article L.34-5 CP&CE.

Bluetooth marketing and the use of contact details of a natural person

A second requirement for Bluetooth marketing to fall under the scope of application of article L.34-5 CP&CE is that the sender makes use of the contact details of a natural person.

For the establishment of a Bluetooth communication and thus for the sending of the message, the sender should process the MAC address and the identifier Bluetooth of the recipient's mobile phone. The question thus consisted in defining whether these technical data could qualify as personal data, i.e. could be acknowledged as "contact details of a natural person".

---

[38] Decision No. 2004-496 DC of 10 June 2004. In this decision, the Constitutional Court faced the question whether e-mail could be acknowledged as private correspondence. The Trust in the Digital Economy Act introduced a technical definition of e-mail messages given by Directive 2002/58/EC. The avoidance of expressly mentioning e-mail as private correspondence in the transposition text has been understood by some parliamentarians as withholding the protection of secrecy of communication from e-mail and thus this matter has been referred to the Constitutional Council. The Constitutional Council considered that the definition contained in the Act, strictly technically speaking, does not restrict or affect the concept of 'private correspondance' and 'secrecy of correspondence as contained in the Act No.91-646 of 10 July 1990 on the secrecy of communications. The competent judge should analyse each case in order to determine whether an email should be considered as private or public communication. The Constitutional Council refers to existing jurisprudence, which had already established a presumption that e-mails are private communication unless their nature made this impossible (Cass. Soc., 2 October 2001, Bulletin 2001 V No.291, p.233.

[39] Cass. Crim., 25 October 2000, Bulletin Criminel 2000 No. 317, p.318.

The CNIL affirms that such is the case without any additional explanation. An analogy could however be made with the doctrine of the CNIL on IP addresses. The CNIL has considered that the concept of personal data, as understood under French law, was very broad and related to any natural person directly or indirectly identifiable, either through an identification number or other elements, including a vehicle plate number, a phone number or an IP address.[40] It follows that, according to the current position of the CNIL, Bluetooth marketing falls under the scope of article L.34-5 CP&CE and thus should comply with the requirements detailed below.

However, as shown by the international debates around the nature of IP addresses and by the fact that some ruling of French jurisprudence has considered that IP addresses were not personal data, this position remains weak. In order to ensure that the phenomenon of Bluetooth marketing indeed falls under the scope of the stringent provisions of article L.34-5 CP&CE, a report to the Parliament on the implementation of the LCEN asked for the regulation of these new practices.[41]

Prior notification to the CNIL

Any collection of personal data should be previously notified to the CNIL. The notification shall comprise an undertaking that the processing complies with the requirements of the law (Article 23 of the Data Protection Act).

Derogations are foreseen when the controller has appointed a Personal Data Protection Official or when the processing meets the requirements to benefit from the derogation of notification as provided by the Simplified Norm on the processing of personal data relative to the management of files of clients and prospects.[42]

7.2.2 Prior consent

Requirements

Article L.34 CP&CE requires previous consent for direct marketing messages when sent by automated means, fax and email. The article also provides for a definition of consent (that is lacking in the French Data Protection Act) that transposes the exact wording of the Data

---

[40] CNIL, *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*, 2 August 2008, available online at : http://www.cnil.fr/index.php?id=2549&tx_ttnews[backPid]=2452&tx_ttnews[pointer]=2&tx_ttnews[tt_news]=332&cHash=7d73167c7a. For further analysis on the debate about personal data in France see COUDERT, Fanny, WERKERS Evi, Note d'observation sous l'arrêt C.J.C.E. (gr. ch.)du 29 janvier 2008: La protection des droits d'auteur face aux réseaux peer-to-peer : la levée du secret des communications est-elle justifiée ?, R.D.T.I. n°30/2008, p.76-85.

[41] J. DIONIS du SÉJOUR and C. ERHEL, *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, 23 January 2008, available online at : http://www.assemblee-nationale.fr/13/rap-info/i0627.asp#P554_97760

[42] CNIL, Délibération n°2005-112 du 7 juin 2005 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25. (Modifiée par délibération n°2005-276 du 17 novembre 2005)(J.O n° 295 du 20 décembre 2005 (Jo électronique), available online at : http://www.cnil.fr/index.php?id=1838

Protection Directive. Consent is defined as « any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed (Article 2.h)".

Consent thus should be free, i.e. expressed by the person itself. Pre-ticked cases should thus be avoided. The E-mailing Code of conduct (UFMD) moreover recommends that consent should not be implicit or "diluted", e.g. based on the approval of the user of the General terms of use. The Charter stresses the importance that the person is aware of consenting to marketing practices. This could be done either by a ticking box, by a rolling menu or the registration to a newsletter. In any case, it should imply a positive act of the data subject. The Code of Conduct of the SNCD also recommends to relying on a positive action of the data subject such as the provision of the email address.

In that sense and as applied to Bluetooth marketing, the CNIL considers that the sending of a message asking the user if he accepts a Bluetooth connection is not sufficient because it happens too late. The CNIL notes that alternative solutions could be used in order to limit the sending of message to the sole persons interested in the information. As a way of example, the CNIL refers to situations where the persons have to put their mobile phones closer to the panel in order to receive the information.

Consent should be specific, i.e. it is only valid towards the controller for the purposes that have been specified. The French Data Protection Act compels for the data to be obtained for specified, explicit and legitimate purposes, and subsequently not to be processed in a manner that is not compatible with those purposes (Article 6). The legitimacy and thus the proportionality, i.e. whether the use of data for marketing purposes is proportionate to the objectives foreseen, of the purposes should be evaluated depending on the nature of the activity of the controller.

It follows from the requirement of specificity that prior consent is required since the first collection of the data for marketing purposes and for each new communication.

Another consequence is that the consent for the transfer to third parties of the personal data for marketing purposes should be object of a specific and separated procedure, e.g. by ticking a second box. In a recent case[43] opposing UFC Que choisir, a French consumer organisation, to Amazon, and dealing with the legality of the Terms of use of the website, the First Instance Tribunal of Paris has deemed the clause authorising Amazon to send commercial offers to users on behalf of other companies to be illicit, despite the opt-out system implemented by Amazon.

Finally, consent should be informed. Information should in particular indicate the identity of the controller. In that sense, article L.34-5 formally prohibits the concealment of the identity of the person on behalf of whom the message is transmitted. Information should also include a) the purpose of the processing, i.e. it should be explicit that the data are collected for purposes of direct marketing; b) the mandatory or facultative nature of the answers; c) the consequences of a lack of answer; d) the recipient or category of recipient of the data; e) the existence of rights of access, rectification, deletion and right to object; f) where relevant, the

[43] T.G.I Paris , 1ère Ch., soc., UFC Que choisir c. Amazon.com et autres, 28 October 2008.

international transfers of personal data toward countries outside the UE. The Charter of the UFMD moreover recommends the use of affirmative sentences.

Derogations to the requirement of prior consent

Article L.34-5 CP&CE only foresees the possibility to derogate to the opt-in system when four cumulative conditions are met:

a) *The data were directly collected from the data subject pursuant to the provisions of the Data Protection Act*. This refers for example to the data minimisation principle. The data to be processed should be adequate, relevant and not excessive in relation with the purpose of the processing (Article 6-3° of the Data Protection Act). It is worth noting that this principle applies also to the collection of personal data that relies on the data subject's prior consent. It also follows that the data should not be stored for a period longer than it is strictly necessary for the purposes for which they were obtained and processed. These periods will usually be linked to a limitation-of-statute period issued from the processing, i.e., the period during which the liability of the controller can be challenged.

b) *The data have been collected in connection with a sale or the provision of services*.

c) *Direct marketing relates to similar products or services provided by the same natural person or legal entity*. The question has been raised as to how the terms "similar services" should be interpreted. Both Codes of Conducts of the UFMD and the SNCD interprets this provision as allowing the promotion of products or services that would fall within the reasonable and legitimate expectations of the clients.[44] The UFMD Code gives the example of a consumer that buys a book to a website offering a large range of cultural services and products. Commercial offers related to any cultural services and products usually proposed by the website are understood to be legitimate. The SNCD Code interprets this wording as products and services with associated or connected uses to the original products or service bought.

d) *The recipient is expressly and unambiguously given an opportunity, via a simple means and at no cost to himself other than the cost of transmitting a refusal, to oppose the use of his details* when they are collected and each time that an electronic mail is sent to him for marketing purposes. (see below 3.4)

7.2.3 The right to object

Article L.34-5 mandates to provide the recipient with a valid means through which he may effectively request the communications to cease, at no cost other than that of transmitting the said request. The SNCD Code of Conduct recommends to inform the user of the identity of the person responsible for the collection of data in order to facilitate the exercise of the right to object.

The Code of conduct of the UFMD recommends to keep an internal and updated list of persons that have shown their opposition to the sending of commercial information from the company or their professional organisations.

---

[44] CAPRIOLI E.A., *Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel*, Etude n°7, Communication Commerce électronique n° 2, February 2005.

As mentioned above, since 2003, specific procedures directed to facilitate the exercise of the right to object to mobile marketing and to fight against mobile spam have been implemented by mobile operators and the French government. Since November 2008, users have a specific short number at their disposal to which they can report mobile spam.

7.2.4 Obligations relative to the content of the message

The sender should clearly indicate to the recipient the commercial nature of the message from the moment of its reception. When it is not technically impossible, e.g. for SMS and MMS, this information should appear in the body of the message.

The sender should also clearly identify the person on which behalf the communication is initiated. As mentioned above, Article L.34-5 CP&CE prohibits the concealment of the identity of the person on behalf of whom the message is transmitted. The SNCD Code of Conduct recommends that the complete identity of the advertiser appears in the electronic message sent to the user or, if it not possible like in a context of mobile marketing, on a website accessible by a simple click. It moreover recommends that the social denomination or trademark of the advertiser appears in the electronic address of the sender or, at a minimum, in the object of the message. It finally recommends that the controller and the owner of the source database, if they are different legal entities, appear both clearly identified in the messages they send or, at a minimum, on the website of reference.

Article L.34-5 CP&CE finally prohibits the reference to an object unrelated to the product or service offered.

7.2.5 The processing of location data

All personal data processing should comply with the general provisions of the Data Protection Act. However, when the location data originate from a public electronic communications network, as it is the case when location data are obtained from mobile devices, supplementary safeguards have been introduced by Article L.34-1 CP&CE that transposes those contained in Directive 2002/58/EC. These safeguards are mainly focused on the consent and information of the subscriber and the user of the service.

Location data are "data allowing the localisation of the user's terminal equipment" (Art. L.34-1.IV CP&CE). Location data will thus always refer to subscribers of the phone number and not to the actual user. Whereas this article does not provide an indication of the data it refers to, Recital 14 of Directive 2002/58/EC provides a list of information included into the concept such as the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded. It thus includes a large range of data that are able to provide a vast amount of information relative to the position and movements of the user.

The processing of location data for marketing purposes will require the prior consent of the subscriber (Article L.34-1 CP&CE). This means that mobile marketing services based on location data should collect the prior consent of the subscriber in addition to the consent given for the processing with marketing purposes. Operators which foresee to offer their own services on the basis of traffic data should obtain the express consent of the data subject. Moreover, the consent can only be given for a limited period which cannot exceed the one required for the provision or marketing of the service.

Article L.34-1.IV CP&CE introduces specific requirements regarding the information to be provided. The subscriber should be informed, before the processing of the location data, of the duration and purpose of such processing and of the transfers of the data to third parties (service providers). This information should also be provided to the user in order to enable him to exercise his right to object to the localisation.

The subscriber should be able to object to the processing of his location data, at any time and free of charge (except for the costs linked to the communication of the withdrawal, as e.g. the cost of the SMS), without having to justify his withdrawal. This article also acknowledges a specific right to the user of the service, when he is a different person from the subscriber, to suspend the consent given by the subscriber, i.e. to deactivate the localisation device.

7.3 Other cases of mobile marketing

Though not falling under the more stringent provisions of Article L.34-5 CP&CE, mobile marketing towards legal persons and without a commercial content should comply with the provisions of the Data Protection Act whenever they use personal data.

7.3.1 Mobile marketing towards legal persons

The wording of article L34-5 CP&CE refers to the use of the contact details of a natural person for direct marketing purposes. The CNIL, as well as French jurisprudence, has qualified email addresses, as long as they contain the identity of a natural person, as personal data. Email addresses such as sav@entreprise.com or contact@entreprise.com do not qualify as "contact details of a natural persons" and thus fall outside the scope of application of article L.34-5 CP&CE.

The CNIL first considered direct marketing making use of any email addresses, as long as it contains the identity of a natural person, even if it was a professional email address, to fall under the scope of article L.34-5 CP&CE. However, after engaging in a discussion with professionals of the sector, the CNIL has reviewed its position.[45]

It now considers that the intention of the law is to protect the privacy of consumers and not to hamper commercial communications between professionals. It follows that direct marketing to professionals will not fall under the provisions of article L.34-5 provided that the content of the message is not related to the professional activity of the recipient. This means that as long as the message sent to this person is related to his function (e.g. promoting software to the person in charge of the computer department), it will fall outside the scope of article L.34-5 CP&CE and will not require his prior consent. In any case, the recipients should have been able, at the moment of the collection of their data, to object to any commercial use of their contact details.

7.3.2 Non-commercial mobile marketing: application of general data protection rules

[45] CNIL, *Position de la CNIL sur la prospection par courrier électronique dans le cadre professionnel*, 2 March 2005, available at : http://www.cnil.fr/index.php?id=1780&news[uid]=238&cHash=161b81f35f

Article 13 of the E-privacy Directive excludes messages sent out by political parties, charities or other organisations, solely expressing views, thoughts and ideas without a direct commercial purpose. Nevertheless, according to Recital 10 and article 1(2) of the E-Privacy Directive these activities are still covered by the general regime of the Data Protection Directive.[46]

In France, the CNIL had to deal with a case of political emails sent to recipients that did not provide their prior consent, nor had been previously informed. [47]

Article L.34-5 CP&CE is not applicable to this canvassing in so far as the message is not intended to directly or indirectly promote goods, services or the image of a person selling goods or providing services constitutes direct marketing. The general data protection rules remain however applicable. The use emails for political marketing should thus comply with the following rules:

- When his data are collected, the data subject should be informed of the fact that his address can be used for purposes of political purposes
- When the data subject receives the message, he should be informed of the origin of the database from which the data are obtained. The data subject will then be able to object to the processing. The message should moreover specify that the political party originating the communication do not have the email addresses at its disposal.
- The recipient should be able to easily object to the processing.

7.4 Conclusion

Transparent mobile marketing practices as the ones advocated by this report are likely to ease the compliance with legal requirements under French Law. Empowering the individuals with tools that enable them to decide upon the processing carried out, to access the data processed, to rectify the inaccurate information and to adjust the data processed to their needs and wishes can only facilitate compliance with the requirements of:

- 'active and specific consent' of the individual (the data subject) for the processing both of the personal data he facilitates and for the processing of his location data. A specific option could be added in order to allow the user to opt for Bluetooth marketing.
- Informed consent of the data subject as he will get additional information upon the exact content of the processing, its purposes and how it works.
- Data minimisation principle insofar as the data subject is the one to define the amount of personal data to be processed. He is the one defining the level of definition of his profile by the software.

---

[46] ASSCHER F. L., HOOGCARSPEL S.A., Regulating Spam, A European perspective after the Adoption of the E-privacy Directive, IT&Law n°10, T.M.C. Asser Press, 2006.

[47] CNIL, *Prospection électronique de l'UMP : la suite…*, 14 April 2006, http://www.cnil.fr/index.php?id=1991&news[uid]=340&cHash=e7c87696ef

- Right to object to the processing. These practices would implement easy ways for the data subject to exercise its right to object to the processing wholly or partly.
- Rights to access rectify and delete the data.

8 Intellectual Rights as Obstacles for the Transparency of Profiling Processes

This section deals with the legal protection by intellectual rights or trade secrets of the profiling processes used in mobile marketing applications and the obstructive effects they can have for the data subject's right to have access to the logic by which his data are processed. We will first assess the principle of transparency of profiling in practices of mobile marketing. The focus will be on the so called rights of access in the European Data Protection Directive and on Transparency Enhancing Technologies. In order to determine how these rights and technologies can become obstructed by intellectual rights or trade secrets, we need to determine which access rights on what legal objects are obstructed. We will focus on databases, computer programs and profiles. In the last section we will assess how these conflicting rights might be balanced by analysing legislative proposals and jurisprudence.

8.1 Transparency of Profiling

8.1.1 The Right of Access to the Profiling Logic

We have already seen in the previous chapters that transparency is an important legal principle that profiling technologies must satisfy. What distinguishes profiling in the context of location based services from other kinds of profiling is the continuousness and pervasiveness of data collection and its unobtrusiveness (Leenes, 2008). The user of location based applications will be even less aware of these processes. This makes the necessity for transparency all the more urgent compared to other kinds of profiling. When personal data are, will, or have been processed in this process the Data Protection Directive offers several tools to achieve this transparency. Article 10 and 11 of the Directive oblige the data controller to provide the data subject with information relating to the identity of the controller, the purposes of processing and recipients of data. This is an important means of making the data subject aware of the fact that he is being profiled.

Apart from obligations for the data controller, the directive also provides the data subject with some rights. Article 12 gives the data subject the right to know which data that are being processed and provides him with the right to rectify, erase or block the processing of such data. In addition it provides him the right to obtain from the data controller "knowledge of the logic involved in any automatic processing concerning him *at least* in the case of automated decisions." What this means is spelled out in article 15 that refers to these automated decisions where every person is granted "the right not to be subject to a decision which produces legal effects concerning him or significantly affects and which is based s*olely* on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." The relation between these articles is, however, not altogether clear. There are important differences to be noted between the protections of these two articles. First article 12 grants a positive right of access to the "data subject", i.e. the natural person whose personal data are processed, whereas the right referred to in article 15 extends to "every person" and is negative in nature: a right not to be subject to automated decisions with significant personal consequences. This right only applies to decisions that are entirely taken on the basis of automatic processing. This means that the right could theoretically already be bypassed when human influences are added to the process of decision making, even if this decision will be wholly based on

automatically generated profiles. We will come back to this point when discussing the German legislative proposal that expands on this issue. In any case, the situation just described does not necessarily imply that the (article 12) right of access to the logic of processing is also bypassed. This right applies *at least* in case the data subject is subject to an automated decision, but is apparently not exhausted by it. In which other situations this right is applicable is not made clear in the directive. In a proposed amendment to the Federal German Data Protection Act the right not to be subject to automated decisions is extended to cases in which no substantial evaluation and judgment has taken place by a human being. This would also extend the right of access to these cases. We will come back to this point later, when we will discuss the amendments. Another question is what kind of right article 15 provides for people who can not be classified as data subjects? What is the status of this right? Is it an enforceable personal right or just a general obligation for the data controller phrased as a personal right?

8.1.2 Transparency Enhancing Tools

The data protection principle of transparency can become embodied in digital code in so-called Transparency Enhancing Tools (TETs). Within FIDIS these TETs have been first worked out in Deliverables D7.7 (Hildebrandt and Meints, 2006) and D7.9 (Hildebrandt and Koops, 2007). They build on the insight that in a world of pervasive data collection and processing, like in the case of location based services, a focus on the protection of personal data alone is not enough. We also have to be protected against the application of profiles to us, which will not always have been created by processing our personal data. TETs provide a precondition for such protection by making the profiling process more transparent to the user. They do so by providing insight in the nature of the profiling process, in the way certain (location) data cause him to be classified in certain profiles and to assess the consequences of such classifications. In FIDIS Deliverable D7.12 (Hildebrandt, 2009) two different types of TETs are distinguished:

Type A: legal and technological instruments that provide (a right of) access to (or information about) data processing, implying a transfer of knowledge from data controller to data subjects, and/or

Type B: legal and technological instruments that (provide a right to) counter profile the smart environment in order to 'guess' how one's data match relevant group profiles that may affect one's risks and opportunities, implying that the observable and machine readable behaviour of one's environment provides enough information to anticipate the implications of one's behaviour.

Type A TETs depend on an exchange of knowledge between data controller and data subject. Note that according to this definition this exchange can either be achieved by a providing the data subject access to data processing or by providing him or her information about this processing. This distinction has important consequences. In the former case of access to data processing intellectual rights or trade secrets in these profiling processes could be at stake. This will be treated in the next section. In the latter case the data subject is especially dependent upon the trustworthiness of the data controller to send him the right information.

Type B TETs give the user the tools to construct counter-profiles. Technologically, there are two ways in which this can be done. FIDIS Deliverable 7.12 describes TETs that externally monitor the behaviour of the profiling system in a certain machine readable environment and that try to anticipate the system's responses. The advantage of this method of counterprofiling is that it does not have to rely on the trustworthiness of the data controller to provide the tools and information necessary for counterprofiling. FIDIS Deliverable 7.9 describes TETs that do rely on this trustworthiness. These TETs need to have access and make use of the same (internal) algorithms and databases that are used by the data controller. It is unlikely that the first "externalistic" kind of counterprofiling TETs will have any consequences in terms of intellectual rights. We will thus mainly focus on the consequences of the second "internalistic" kind of TETs.

Type B TETs will need to have access to machine readable data from the user's environment (indicating the potential consequences of profiling). Since within mobile marketing services the workflow of data processing is highly distributed, different factors have to be taken into account. In order to make a reliable counter-profile TETs will need to have access to location data.[48] These data are generated by (a combination of) different kinds of technologies like satellite based position systems, sensors based systems, wireless networks, cell-based mobile networks, RFIDs or chip card based payment devices. The data located in devices is sent to sensors which transmit the information to backend systems of the mobile operator, which interpret and use this information. In case of mobile marketing the results of this processing will then be sent to the provider of these location based services (LBS) who will use or further process these data to provide a service.[49] For type B TETs to work effectively they would thus need to receive location data either from devices or from sensors (which then need to be transmitters as well). They would also need to access and make use of the software linking the collected data and to the software used by both the mobile operator and the LBS provider to analyse the data.[50] These actions might imply the making of copies of software or the extraction of data from databases, which could be blocked by exclusive intellectual rights or trade secrets on these objects.

8.2 Intellectual Rights in Profiling Processes

The conflict between these two legal regimes is central to this chapter. In order to assess how to balance these two conflicting legal regimes, we have to first investigate what this blockade exactly consists of. It is therefore necessary to determine the regime of protection applicable to the legal objects that can be identified within profiling processes. In Deliverable 7.16 a first assessment has been made of the legal status of profiling processes. It identified three relevant legal objects of protection, which are: databases, profiling software and the profiles themselves. Databases can be protected by copyright or a *sui generis* right. Software can be protected by copyright or patents. Profiles might be protectable by copyright or otherwise by trade secrets. This section will follow and expand on the analysis of Deliverable 7.16.

[48] Since in the majority of cases these location data can be related to an identified or identifiable natural person, they will often be personal data triggering the data projection regime of Directive 96/9/EC.
[49] See the descriptions in FIDIS Deliverables 7.2 and 7.5 for more detailed information about these technologies.
[50] Compare the analysis of Hansen *et al*. 2007 of the distribution of the workflow in digital environments.

8.2.1 Databases

The first potential legal objects at stake are databases. Does the data protection directive grant the data subject the right of access to the data controller's databases in which his data are stored? Section V of the Directive speaks of "the data subject's right of access to data" and the name of article 12 is "rights of access". When we have a closer look at how the specific right is actually coined, these formulations might be quite misleading. The data subject is granted the right to obtain from the controller "communication to him in an intelligible form of the data undergoing processing and of any available information as to their source." The article thus grants the right to be *communicated* information about his data, but this does not mean he has *access* to his data as they are stored in the databases of the data controller or a third party. This makes it unlikely that intellectual rights on databases might be breached in this process.

This might be different in the case Transparency Enhancing Tools are used. Let us have a look at the two types of TETs distinguished earlier. It was mentioned that type A TETs provide access to, or information about data processing, implying a transfer of information from data controller to data subjects. As we have seen the distinction between providing access, or communicating information about data processing is very relevant from an intellectual rights perspective. An assessment of the current type A TET's shows that they mostly rely on information being communicated from the data controller to the data subject.[51]

In case of TETs of type B the situations is more complicated. The answer to the question whether access to the database of the data controller is needed will depend on how the TET functions. When the TET only externally monitors the behaviour of the profiling system combining it with machine readable data of the environment there will not be an IR problem, since no access to databases, algorithm or profiles of the data controller is required. In case internalistic TETs are used, which do need this kind of access, we have to investigate whether this access might compromise intellectual rights.

According to the Database Directive (96/9/EC) databases can be protected by two kinds of intellectual rights: copyright and the *sui generis* database right. Copyright can be vested on a database when the "selection or arrangement" of data constitutes the "author's own intellectual creation".[52] Copyright on databases protects only the expressive structure of the database not its informational contents.[53] These contents thus might be accessed or extracted, as long as the way they are selected or arranged is not appropriated. When TETs would extract data in this manner copyright is not infringed and could not be used to block a data subject's right of access.

The *sui generis* right applies to databases the making of which required a "substantial investment in either the obtaining, verification or presentation of the contents".[54] When this is the case, the maker of the database has the right to prevent extraction or re-utilisation of the database or substantial parts of its contents. Reutilisation refers to the transfer of the database to another medium; reutilisation refers to making the database available to the public. When externalistic type B TETs are to base their counter-profiling on the same massive amounts of data which generated the marketer's group profiles, extraction, or, at least access will be

---

51 See section 5.1.2 of FIDIS 7.12

52 Article 2(1) Directive 96/9/EC

53 Article 5 in combination with article 3 (2) Directive 96/9/EC

54 Article 7(1) Directive 96/9/EC

required. Here we thus have a potential clash between the functioning of TETs and intellectual rights.

8.2.2 Profiling Software

The second object in profiling processes in which intellectual rights could be vested are the computer programs used for profiling. Does the data protection directive grant the data subject the right of access to these programs? The relevant right in article 12 (a) is inscribed under the header "the data subject's right of access to data" of Section V of the data protection Directive. Once again a closer look at the formulation of the specific right casts some doubt. The data subject is granted the right to obtain from the controller "knowledge of the logic involved in any automatic processing concerning him from the data controller." The article thus grants the right to *obtain knowledge* of the *logic* involved and not necessarily the right of *access* to the *computer programs* used. Two important distinctions have to be made here between access and communication and between logic and computer programs. These render four possible situations which all have different consequences from an intellectual rights perspective:

1. Communication of information about the processing computer program
2. Communication of information about logic of processing
3. Access to the processing computer program
4. Access to the logic of processing

If to "obtain knowledge from the data controller about" the profiling logic (2) or software (1) means the same as "be communicated information about" then no intellectual rights are at stake. No copies of the computer programs used for offering the location based services have to be made or distributed, leaving aside the question if this would be technologically feasible at all. When it is however read as a right of "access to" the profiling logic (4) or the computer program (3) intellectual rights could be involved. The difference in point 3 and 4 between the concepts "logic" and "computer program" could also have importance from a perspective of intellectual rights. In order to assess these differences, we have to take a closer look at intellectual rights on computer programs.

According to Directive 91/250/EC those computer programs that are "original", constituting "the author's own intellectual creation", merit protection by copyright.[55] The author of the protected programs has the exclusive right to reproduce the computer program and the right to distribute it to the public.[56] Article 4(a) further states that "insofar as loading, displaying, running, transmission or storage of the computer program necessitates such reproduction, such acts shall be subject to authorisation by the right holder." Since technologically speaking a right of access to a computer program will come down to one of these acts, it will be covered by the reproduction right and thus constitute a potential obstacle. This also shows that both the TETs of type A, which provide access to the computer programs used for data processing, as externalistic TETs of type B, which base their counterprofiling on these programs, fall under the scope of this exclusive right and can be blocked.

With respect to this potential conflict recital 41 of the Directive states that "the right to know the *logic* involved in the automatic processing of data concerning him [...] must not adversely affect trade secrets or intellectual property rights in particular the copyright protecting the

55 Article 1(3) Directive 91/250/EC
56 Article 4(a-c) Directive 91/250/EC

software". We here again see the distinction between logic and software programs reappear. It seems to state that the data subject has the right to know the logic of processing and not so much the computer program itself. This distinction is relevant within a framework of intellectual rights. In accordance with general copyright principles copyright protection extends to the particular expression or form given to a computer program and not to the underlying ideas and principles.[57] Recital 14 of Directive 91/250/EC elucidates this point by stating that "to the extent that *logic*, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected".[58] This is an unclear statement. It does not say anything about the status of the logic, algorithms and programming languages themselves. This point needs further elucidation by the ECJ. In our context this is of crucial importance. When the logic of processing underlying the computer program is excluded from protection, there is no copyright barrier for the right of access. When this logic or these algorithms are covered by copyright protection, access could be obstructed or be restricted to the ideas and principles "comprised" by them.

Computer programs that can not be copyrighted for a lack of originality can always be protected by know-how protection. This regime will only protect the right holder against certain specific illegal actions by employees (trade secret), competitors (unfair competition law) or other legal subjects. A trade secret offers a company protection by making disclosure by employees an offence of criminal law. We have seen that recital 41 also mentioned that computer programs protected by trade secrets could not be used as an absolute block against the access rights of the data subject.

8.2.3 Profiles

The last object in profiling processes which might be relevant in our context is the profile itself. Does the data protection directive grant the data subject the right of access to these profiles? And, if so, are there intellectual rights in profiles which could be obstructing such access? We can be relatively short on this topic. Firstly, the Data Protection Directive does not offer an explicit right of access to profiles or a right to be communicated information about profiles. Second the legal status of profiles is yet unclear. Some research is being conducted on this topic (Custers (ed.), 2009; Van Dijk, 2010). The preliminary findings are that in some cases profiles might receive copyright protection as "compilations of data". This will however depend on several factors like the mode of representation of the profile, the kind of algorithms used, whether supervision of the profiling process has taken place and the originality of the profile.

This would thus require a closer look at the specific profiling method and process employed by a provider of mobile marketing services. In classical geodemographic systems clustering, factor analysis and regression algorithms are used. Recommender systems use search based methods, clustering or collaborative filtering. These are all deterministic algorithms. For copyright purposes this implies that the expressive form of the resulting profile could possess sufficient ties with the "own intellectual creation" of its maker to classify as an original work (this is not possible when probabilistic algorithms are used). To judge if this is also the case in the practice of marketing profiling has to be determined by an empirical analysis of the concrete profile and its process of construction. The same goes for the assessment of the

57 Article 1(2) Directive 91/250/EC
58 Recital 14 Directive 91/250/EC

originality. When a profile cannot be copyrighted (either in theory or in practice) it can be protected by making it a trade secret.

8.3 Striking a Balance

The framers of the Data Protection Directive have realised that there could be potential conflicts between the right of access and intellectual rights. The already mentioned recital 41 of the Directive stated that "the right to know the logic involved in the automatic processing of data concerning him [..] must not adversely affect trade secrets or intellectual property rights in particular the copyright protecting the software". It is not clear how such "adverse effects" should be interpreted in balancing the right of access and these intellectual rights. The recital just adds that "these considerations must not, however, result in the data subject being refused all information." This seems to confirm that in fact we are not speaking about an access right, but a right to be informed. The statement implies that the data controller cannot use intellectual rights as an absolute block against this right, meaning that he should provide the data subject with *some* information. Arguably this information should be sufficient to form adequate "knowledge of the logic of processing".

8.3.1 The German Legislative Proposal

This section will shortly address the current debate in the ongoing legislative process on profiling practices in credit scoring in Germany. Presently two amendments to the Federal Data Protection Act are debated in Germany. The draft bill referring to profiling and scoring practices including an overview of the conflicting interests brought forward by different lobby groups will be presented in FIDIS Deliverable D7.16 (Custers, 2009) and builds on the analysis in FIDIS Deliverable 7.12 (Hildebrandt 2009).[59] The draft bill is a response to the lack of transparency in scoring practices in financial institutions, because of which the data subject is no longer capable of checking how credit decisions came about. As a solution the amendment strengthens the data subject's rights to be informed. The two changes which are relevant for our purposes are the changes to §§ 6a and 34 BDSG.

The amendment clarifies when we can speak of automated decisions and the scope of the information to be communicated. The legislator says that the goal behind § 6a (1) BDSG, which prohibits decisions exclusively taken on basis of automated processing, is to give the data subject the possibility to expose his standpoint to a human and to test these automated decisions. A decision will especially be considered to be exclusively based on the automated processing of personal data, when no evaluation by a natural person of its content and the decision based on it has taken place. This entails that this prohibition cannot be circumvented when the decision taken only requires more or less formal editing or processing by a human who does not have the capability to deviate from it. The new provision applies both to automated processes which irrevocably dictate a certain decision as well as to the processes that have essentially prepared the decision.

The amendment includes several new rights to be informed in a new § 34 (2) BDSG. It states that in the case of a credit-scoring calculation, the institution responsible for making the (credit) decisions has to *provide* the data subject upon request with the current credit scores

[59] Section 5.3.2

and those processed within the recent time, the type of data processed and an understandable explanation of the constitution of the individual probability score. This is a considerable expansion of the right to be informed. In terms of the analysis of intellectual rights made in the previous sections the credit score refers to the (personal) profile and the constitution of the probability score refers to the algorithm or computer program used. Since the article speaks of "provision" to (*erteilen*) the data subject we are again not dealing with an access right.

With regard to the issue of a potential clash with trade secrets or intellectual rights in the score algorithms, the legislator states that section § 34 (2) BDSG "constitutes the duty to explain the constitution of the probability score in the specific case in an easy and generally intelligible form. This ensures that on one hand companies *do not need to reveal the underlying score algorithm* as they have an *overriding legitimate interest* regarding it's protection, and that on the other hand the *facts* on which the probability calculation is based must be revealed to the data subject upon request in a way lay people can understand. Thus, no complex mathematic formulae need to be revealed, especially as they are not generally understandable. Rather the data subject must be put in a position to understand the *underlying facts* resp. the *relevant circumstances*. The result must always be comprehensible to the data subject to the extent that she can properly exercise her rights, reveal possible mistakes in the basis of calculation and explain deviations from the automatically gained typical rating of the underlying facts."[60]

Here we see a clear balance of interests. The scoring algorithm or computer program will not have to be revealed, because the data controller has an overriding interest in its protection. Copyright and trade secrets here prevail in the balancing act. Since the data subject should not be refused all information, the constitution of the probability score should be explained to him by revealing to her the underlying facts and relevant circumstances. We have seen that facts or ideas underlying computer programs, logic or algorithms are not protected by copyright. The conflict here has been removed and is further justified by the fact that a lay data subject will not even understand these complex mathematical formulas. In our context this argument does not hold however against a data subject empowered with transparency enhancing technologies. The TETs will do the "understanding" on behalf of the data subject who is just fed back the results.

The information rights of § 34 (2) BDSG explicitly only refer apply to practices of credit scoring. They cannot be applied to profiling in marketing or location based services. They do elucidate however how a sector tailored balance can be struck. Let us now look at other examples in the jurisprudence.

8.3.2 Jurisprudence

We can also find a few examples of sector tailored balances struck by courts or governmental institutions. In this section we will have a look at three relevant cases

- The decision of the European Court of Human Rights in the case Gaskin vs. UK
- The decision of the Dutch Court of Cassation (HR) in the Dexia cases
- An advise by the Dutch Data Protection Comity (CBP) to the NIT

[60] http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2008/0501-600/548-08,templateId=raw,property=publicationFile.pdf/548-08.pdf

Gaskin vs. UK

The Gaskin case is not directly about a conflict between the right of access and intellectual rights, but instead between access rights and confidentiality. The case was about a British citizen who spent the majority of his childhood in care. The applicant wanted to have access to certain confidential records compiled by local authorities relating to him and the time he spent in care. He wanted to know details about were he was kept, by whom and in what conditions in order to learn about his past. The authorities refused on the basis that disclosure would be contrary to the public interest of maintaining an efficient child care system. This system owes its efficiency to the fact that the principal contributors to the records can do so in strict confidence. The judge thus had to strike a balance between the applicant's private interest of access to case records relating to him and the public interest of maintaining an efficient child care system.

The Court decides that: "persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can in principle be considered to be compatible with the obligations under Article 8, taking into account the State's margin of appreciation. The Court considers, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case."[61]

We here see that the public interest in confidentiality of records can prevail over the right to access, only when in accordance with the principle of proportionality: the refusal should be in proportion to the potential consequences of disclosure. This means that an independent authority or procedure should be available to test or check whether the conditions for confidentiality have been fulfilled.

Dexia Bank

The Dexia case is about a customer of the Dexia bank who wants access to his personal file to judge how Dexia has estimated his financial situation and experience as a stock-broker.[62] Dexia provides a general summary of the personal data used. Article 35 of the Dutch Data Protection law (WBP) determines that the communication of data has to provide a "complete" oversight of the processing. The central question for the Dutch High Court of Cassation is about the scope of the right of access in this article. The Court judges that the data controller cannot limit itself to providing global information to the data subject. In order to effectively make use of the right of control and correction, the data subject needs sufficient insight in his data and the way they are processed. This means that the oversight needs to be specific, since the informational value might otherwise be lost. The exact context in which data are

[61] ECHR, *Gaskin v. UK*, Application no. 10454/83, 7 July 1989, para. 49.
[62] See the analysis of this decision in De Hert *et al.* (2007).

processed could be crucial for this. The data subject does not need a specific interest in obtaining the information. This interest is presupposed by data protection law. Interesting is that the Court of Appeal had earlier judged that Dexia had to indicate whether it had made a risk profile of the client based on personal information relating to his financial position, his experience as a stoke broker and his goals. If this is the case it would have had to provide the client with a copy of the profile. Dexia also needed to indicate whether it had made an estimate of the client's credit worthiness and, if so, also would have had to provide a copy. Dexia's complaints against these stipulations were rejected in the ruling by the Supreme Court. An estimation of a client's credit worthiness is probably based on group profiling on the basis of data of other persons. The Article 29 Working Party has determined that when a group profile is applied to individual cases it is to be treated as personal data.

In this case we thus see a strong context-related component to the right to be informed. It also shows that the data subject does not need to state a specific interest for exercising the right of access. This might be important in the case of mobile marketing. The case further demonstrates a right of access to personal profiles and group profiles applied to individuals.

Institute for Psychologists (NIT)

The case is an answer by the Dutch Data Protection Authority (CBP) to a request for an advice of the Dutch Institute for Psychologists (NIT) about a client's right of access to data about psychological tests they took.[63] This is the only case where intellectual rights explicitly figure. The question was whether the copyright on psychological tests and the fact that the test loses value when questions and answers are made public, can be a reason for limiting the right of access. With regard to the latter impact the NIP thinks that providing these data will seriously damage the interests of the profession. It enhances the risk that the data will become public. Answers could then be practiced in advance, which will negatively influence the reliability of the test results. The authors of the tests also think that providing a copy of the test infringes their copyright for which they do not give permission. The CBP judges the legitimacy of limiting the right of access in this case, in the light of three criteria extracted from article 8(2) EVRM:

1. The limitation of the access right by not providing a copy has to be *necessary* for the protection of the value of the tests as valid instruments or for observing the copyright of the right holder.
2. The interference in the private life of the person involved that is the result of not giving the copy, has to be *proportionate* to the possible consequences of providing the copy.
3. The negative consequences of providing the copy could not have been avoided in another less intrusive manner.

The CBP states that the goals of copyright and data protection are in conflict. Whereas copyright prohibits the provision of the copy, data protection law obliges such provision in case of a request for access. It acknowledges the balance mentioned in recital 41 of the Data Protection Directive which needs to be found between the two conflictive regimes. It judges that the interests of the profession legitimate a refusal to provide access to psychological tests. A reasonable balance is struck when the information provided is limited to a supervised access of the personal data during a meeting and a written final report that

[63] Letter of CBP to NIT, 15 July 2008, at http://www.cbpweb.nl/downloads_overig/NIP.pdf

contains the outcome of the test. We again see that the balance between the right of access and intellectual rights takes account of the specific interests in each context.

8.4 Conclusion legal safeguards

Data of someone using location based services are continuously and pervasively collected and can be used for increasingly specialised and personalised marketing offers. The person in question will be barely aware of these ubiquitous underlying profiling processes. This makes the necessity for transparency all the more urgent. Such transparency can be achieved both by legal and technological tools. We concluded that the transparency rights provided in article 12 of the Database Directive are not "access rights" but rights to be provided with information. Transparency Enhancing Technologies (TETs) are a way of technologically affecting transparency. These technologies may however require access to the profiling processes.

Intellectual rights or trade secrets within profiling processes can block the data subject's attempts to achieve transparency. Relevant in this obstructive sense are the *sui generis* database right, copyright on software and trade secrets on profiles. It can be preliminarily concluded that these rights in their present form constitute a serious problem for TETs based on access to profiling processes. With regard to the right to be informed, a balance needs to be struck between these conflicting regimes. This balance needs to ensure that the data subject will not be refused all information. The information the data subject is to receive should at least be sufficient to empower him to use his control rights effectively. In the case of mobile marketing this entails that the data subject has to be informed about the personalised profile that the marketing offers are based upon and about the facts and circumstances that constituted this profile.

9 Summary, Findings and Further Work

This chapter provides a summary of the issues discussed in this deliverable as well as a collection of findings and a list of items for further work.

9.1 Summary

Based on the results of FIDIS Work Package 7 on Profiling and Work Package 11 on Mobility and Identity the report at hand provides a multifaceted view on the topic of mobile marketing. Results of both Work Packages represent the theoretic framework of this investigation. The construct of transparency was a central element within this deliverable, combining economic, technical, and legal perspectives on mobile marketing.

As described in Chapter 2 (Introduction) advanced mobile marketing processes collect many identity relevant data and match them when creating individualised mobile marketing contents. The different chapters of this report focussed on parts of this process. Methodologies, motivated by their potential impact on user acceptance, were proposed in order to design mobile marketing in a more privacy preserving and transparent way. Legal regulations applying on different parts of the process were described to demonstrate the importance of users' compliance with regard to the usage of personal data, and potential conflicts of interest between users and providers of mobile marketing applications were described. In particular, the deliverable focused on the following topics (see Figure 11):

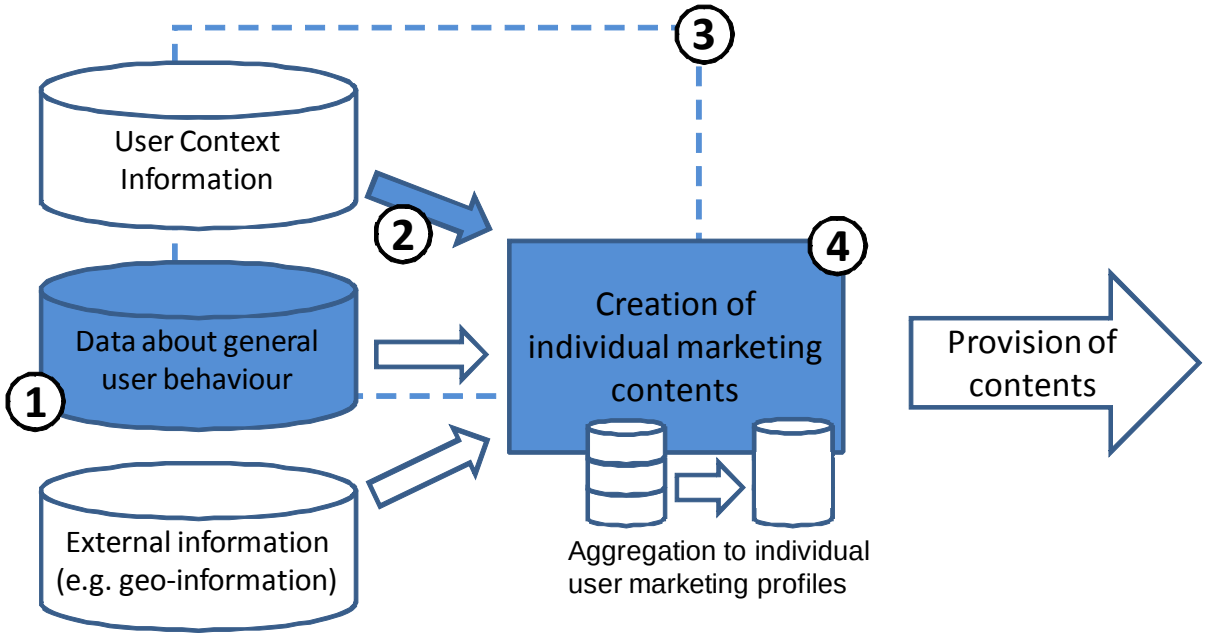

Figure 11 Aspects addressed

1) **Chapter 3** focused on the process of collecting data about general user behaviour: Having a look at the process of creating individualised marketing contents, the knowledge about users' interests, behavioural patterns, and attitudes towards incentives is a necessity, in order to customise services in an efficient way. Classically, data mining techniques are employed in order to detect this kind of information. Chapter 3 has shown how data mining can take place while respecting the private sphere. This can also contribute to raising users' acceptance of mobile marketing applications.

2) Designing mobile marketing in a transparent way by explaining users' what data is collected, processed and stored has been discussed in **Chapter 4**. Entering into an active dialogue between providers and recipients of mobile marketing services can help to raise the services' quality. This has been demonstrated using the example of mobile recommendations.
3) The legal framework applying on different parts of the process of creating individualised mobile marketing contents has been described in **Chapters 5 to 7**. In respect to the legal requirements transparency is a central principle and necessary for compliance of any form of location based marketing. The necessary consent is a central means to ensure the users' knowledge that the recommendation system requires processing of personal and location data. This holds to be true for the German and French law and will, as the central rules are based on European Directives, hold true for other EC jurisdictions as well. Informed consent is required by a set of parallel regulations. For the area of location data specialised rules based on the E-Privacy Directive apply. Besides these the general rules of the Data Protection Directive apply for other personal data processes such as the user's profiles on interests. The Data Protection Directive also ensures the right of access in respect to data processed and to a certain extent to the logic of processing.
4) Transparency in the process of creating individualised contents can be related to conflicting interests between the involved parties. Intellectual rights or trade secrets on the providers' side and users' attempts to achieve transparency are an example for that. **Chapter 8** especially focused on this aspect.

9.2 Findings

Classic mobile marketing was not necessarily dependent on identity related data beyond users' telephone numbers. This has changed, and mobile marketing is now very relevant for the future of identity in the information society due to several reasons:

- The pressure for more efficient mobile marketing that targets customers more precisely causes the need for more and more identity related data to be used in mobile marketing processes. When profiling of users is applied the respective profiles and algorithms get ever more complex to deal with the rising amount of context data.
- The ability to identify "real" users on an individual basis rises, as mobile devices are in most cases used by the person whose "real" identity is connected to the SIM Card via a contract. Profiles created for marketing purpose can hence be connected to users' actual identity.
- In contrast to other marketing tools, mobile marketing is characterised by a large and growing amount of available context information, including users' local context.
- The tension between the large amount of data being collected by mobile marketing processes and marketing's aim for building positive customer relations makes it all the more important to bring privacy preserving and transparency enhancing mechanisms into place.

9.3 Further Work

Within this deliverable we demonstrated how to preserve privacy and enhance transparency in different parts of the mobile marketing process, which legal regulations are applied and what conflicts of interest might arise. Nonetheless, further work is needed. One core topic to this regard is transparency:

- The creation of transparency as discussed at the example of mobile recommendations might not apply to every other type of mobile marketing application, as users profit from a

high degree of personalisation in mobile marketing in a very direct way. Therefore the relevance of transparency for mobile marketing applications in general needs to be researched further.

- The discussion of transparency in Chapter 4 was restricted towards transparency of directly collected and processed context information. This should be developed further to consider identity information that can be derived by matching actual context information with external data as e.g. geo data.
- As the processing of personal data in advanced mobile marketing and profiling applications gets more and more complex, the need for transparency cannot simply fulfilled by getting access to the data being stored: Additional information on how the data are processed is needed.
- The request for transparency in profiling requires providers to disclose central parts of their business logic, leading to conflicts with the protection of their intellectual property rights. This needs to be balanced with users' claims for their right to be informed.

Another core topic that should be addressed is the protection of users' identities throughout the complete process of creating individualised mobile marketing contents.

- Users need to enabled to remove the data they once disclosed to providers of mobile marketing applications.
- The concept of pseudonymity should be operationalised in a much broader way than it is presently in the area of mobile marketing.
- Users should be given the legal safeguards as well as the technical ability to protect their identity by using pseudonyms when disclosing personal data.
- Intermediaries have to be brought into place in order to achieve pseudonymity in mobile marketing applications.

Research has already been performed on these topics on a technical driven level e.g. within the PRIME project[64]. Nonetheless, the diffusion of this kind of technologies tying into the application logic of application providers such as mobile marketing providers is still at an initial stage. The following approaches are considered to be another precondition for protecting users' identity by means of pseudonymity in mobile marketing applications:

- The diffusion of technologies protecting users' identity information by pseudonymity is to be researched in more detail.
- Business processes and models have to be adapted and developed further to allow for protecting users' identity information by pseudonymity.
- To support the protection of users' identity in highly personalised marketing applications policy makers should strive for giving the right incentives in order establish mechanisms as laid out and described within this deliverable.

This also holds true and may even apply all the more on emerging marketing methodologies trying to address customers' interests on an increasingly precise level.

[64] See https://www.prime-project.eu/.

10 Bibliography

Albers, A., *An Electronic Market Framework for context-sensitive Mobile Consumer Profiles in the Marketing Domain*. AMCIS, Keystone, USA August 2007.

Agrawal, R., Srikant, R., 'Privacy Preserving Data Mining', Proc. ACM SIGMOD Conf. Management of Data, pp. 439-450, May 2000

Asscher, F.L., Hoogcarspel, S.A., 'Regulating Spam, A European perspective after the Adoption of the E-privacy Directive', *IT&Law* n°10, T.M.C. Asser Press, 2006.

Awad, N.F., Krishnan, M.S., 'The Personalization Privacy Paradox: An Empirical Evaluation Of Information Transparency and the Willingness to be Profiled Online for Personalization', *MIS Quarterly*, Vol.30, No. 1, 2006, pp.13-28.

Balabanović, M., Shoham, Y., 'Fab: content-based, collaborative recommendation'. *Communications of the ACM*, Vol.40, No.3, 1997, pp. 66-73.

Bilgic M., Mooney, R.J., 'Explaining Recommendations: Satisfaction vs. Promotion, Beyond Personalization', *A Workshop at the International Conference on Intelligent User Interfaces*, San Diego, CA, January 2005.

Bleicher, J.K., Hickethier, K., *Aufmerksamkeit, Medien und Ökonomie*. Lit, 2002

Bødker, S., *Through the Interface – a Human Activity Approach to User, Interface Design*, Dissertation, Aarhus University 1987.

Bramhall, Pete (ed.) PRIME deliverable D.4.2.b: *Evaluation of final application prototypes*, 2008, online: https://www.prime-project.eu/prime_products/reports/eval/cnf_del_D4.2.b_pt_wp04.2_V7Final.pdf

Berson, Alex, Smith, Stephen, Thearling, Kurt, *Building Data Mining Applications for CRM. McGraw-Hill Companies*, 1999, ISBN 0071344446.

Caprioli E.A., Loi du 6 août 2004. 'Commerce à distance sur l'Internet et protection des données à caractère personnel', *Communication Commerce électronique* n° 2, Etude n°7, Février 2005.

Chor, B, Goldreich, O., Kushilevitz, E., and Sudan, M., 'Private information retrieval', in *Proceedings of the 36th Annual Symposium on Foundations of Computer Science (FOCS'95*), page 41, Washington, DC, USA, 1995. IEEE Computer Society.

Coudert, F, Debet A., De Hert P.,'Chapter 4: Constitutional Rights and New Technologies in France', in *Constitutional Rights and New Technologies. A comparative study'*, eds. Koops, B.J., Leenes, R. and De Hert, P., IT&Law n°15, TMC Asser Press, The Hague, 2008.

Coudert, Fanny, Werkers Evi, 'Note d'observation sous l'arrêt C.J.C.E. (gr. ch.) du 29 janvier 2008: 'La protection des droits d'auteur face aux réseaux peer-to-peer : la levée du secret des communications est-elle justifiée ?', *R.D.T.I.* n°30, 2008, p.76-85.

Cuijpers, C., Roosendaal, A., Koops B.-J., Fidis deliverable D11.5, *The legal framework for location-based services in Europe*, Frankfurt am Main, 2007

Custers, B. (ed.), Fidis deliverable D 7.16: *Profiling in Financial Institutions*, Frankfurt, 2009 (to be published)

Dahlen, B.J., Konstan, J.A., Herlocker, J.L., Good, N., Borchers A., Riedl, J., *Jump-starting movielens: User benefits of starting a collaborative filtering system with "dead data"*, University of Minnesota TR 98-017, 1998.

De Hert, P., Hildebrandt, M., Gutwirth, S., Saelens, R., *De WBP na de Dexia-uitspraken*, P&I, 4, 2007

Donaldson, J., 'A Hybrid Social-Acoustic Recommendation System for Popular Music' *Proceedings of the ACM Recommender Systems*, Minneapolis, Minnesota, USA, 2007, pp. 187-190.

Dreier, T., Hugenholtz, B. (eds.), *Concise European Copyright Law*, Kluwer Law International, Alphen a/d Rijn, 2006

Eui-Hong, H., Karypis, G., 'Feature-based recommendation system', *Proceedings of CIKM*, 2005, p.446-452.

Figge, S., ‚Innovatives Mobile Marketing - Kontextabhängige Kundenansprache mit Hilfe mobiler Portale', in: Rannenberg, Kai (Hrsg.): *Schriften zum Mobile Commerce und zur Mobilkommunikation*; Hamburg 2006.

Franck, G., *Ökonomie der Aufmerksamkeit*. Carl Hanser; 1998.

Frese, M., 'A Theory of Control and Complexity: Implications for Software-Design and Integration of Computer Systems into the Work Place, in: Frese, M., Ulich, E., Dzida, W. (Hrsg.), *Psychological Issues of HCI in the Work Place*. Elsevier Science, Amsterdam, 1987, pp. 313-337.

Fritter, M., 'Towards More "Natural" Interactive Systems', *International Journal of Man-Machine Studies*, 11, 1979, pp. 339-350.

Fu, X., 'Evaluating Sources of Implicit Feedback in Web Search'. *Proceedings of the ACM Recommender Systems*, Minneapolis, Minnesota, USA, 2007, 191-194.

Hansen, M., Hansen, M., Häuser, M., Janneck, K., Krasemann, H., Meints, M., Meissner, S., Raguse, M., Rost, M., Schallböck, J., *Verkettung digitaler Identitäten*, Study Commissioned by the Federal Ministery of Education and Research, Germany, 2007

Hefermehl, W., Köhler, H. Bornkamm J. (eds.), *Gesetz gegen den unlauteren Wettbewerb: Preisangabenverordnung Unterlassungsklagengesetz*, München, 2009

Herlocker, J.L,. Konstan, J.A., Riedl, J., 'Explaining collaborative filtering recommendations', *ACM conference on Computer supported cooperative work*, 200, pp. 241 – 250.

Hildebrandt, M. (ed.), Fidis deliverable D 7.12: *Behavioural Biometric Profiling and Transparency Enhancing Tools*, Frankfurt, 2009, online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf

Hildebrandt, M., Meints, M. (eds.) Fidis deliverable D7.7: *RFID, Profiling, and AmI*, Frankfurt, 2006, online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf

Hildebrandt, M., Koops, B.J., (eds.), Fidis deliverable D7.9: *A Vision of Ambient Law*, Frankfurt, 2007, online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf

Hill, W.C., Stead, L., Rosenstein, M., Furnas, G.W., *Recommending and Evaluating Choices in a Virtual Community of Use*, CHI 1995, pp. 194-201.

Hingston, M., *User Friendly Recommender Systems*, University of Sydney, School of Information Technologies, 2006.

Jaideep Vaidya, Chris Clifton, Michael Zhu, Christopher Wade Clifton, *Privacy Preserving Data Mining*, Springer, 2006, ISBN 0387258868.

Jung, S., Herlocker, J.L., Webster, J., 'Click data as implicit relevance feedback in web search', *Information Processing and Management*, 43, 3, 2007, pp. 791-807.

Kamp M., Weichert T., *Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken der Verbraucher,* Kiel, 2005 Available at: http://www.bmelv.de/cln_045/nn_749972/SharedDocs/downloads/02-Verbraucherschutz/Markt/scoring.html__nnn=true

Kelly, D., Teevan, J., 'Implicit Feedback for Inferring User Preference: A Bibliography, *SIGIR Forum*, Vol.37, No.2, 2003.

Koenemann, J., Belkin, N., 'A case for interaction: A study of interactive information retrieval behavior and effectiveness', in *Proceedings of the Human Factors in Computing Systems Conference*, NY, 1991.

Konstan, J.A., Miller, B.N., Maltz, D., Herlocker J.L., Gordon, R., Prairie, E., Riedl, J., 'GroupLens: applying collaborative filtering to Usenet news', *Communications of the ACM*, Vol.40, No.3, 1997, pp. 77 – 87.

Kosta E., Valcke P., Stevens D., 'Spam, spam, spam, spam… Lovely spam!' Why is Bluespam different?', *International Review of Law, Computers and Technology*, Manuscript accepted in July 2008, *In press*

Kotler, P., and Bliemel, F., *Marketing-Management*, Schaeffer-Poeschel, Auflage10., überarb. und aktualisierte Aufl, Stuttgart, ISBN: 9783791016894, 2001.

Leppäniemi, M., Sinsalo, J., Karjaluoto, H.: Mobile Maerketing Research (2000-2005): Emergence, Current Status, and Future Directions, In Proceedings of the CMC 2006, 11th Conference on Corporate and Marketing Communications, pp. 85-93, Ljubljana, Slovenia, April 21-22, 2006.

Leenes, R., 'Reply: Mind my step?', in Hildebrandt M, Gutwirth S (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Springer: Dordrecht, 2008

Linden, G., Smith, B. and York, J., 'Amazon.com Recommendations: Item-to-Item collaborative filtering'. *IEEE Internet Computing*, 7, 1, 2003, pp. 76 –80.

Maaß, S., *Transparenz. Eine zentrale software-ergonomische Forderung*, Report Nr. FBI-HH-B-170/94, Hamburg, 1994.

Maaß, S., 'Why Systems Transparency?', in Green, T.R.G., Payne, S. J., van der Veer, G. C. (Hrsg.). *The Psychology of Computer Use*. Academic Press, London, 1983, pp.19-28.

van Meteren, R., van Someren, M., *Using Content-Based Filtering for Recommendation*, University of Amsterdam, Netherlands, 2000.

Muramatsu, J., Pratt, W., 'Transparent Queries: investigation users' mental models of search engines', *ACM SIGIR conference on Research and development in information retrieval*, New Orleans, Louisiana, United States, 2001, pp. 217 – 224.

Nguyen, Q.N., Ricci, F., *User Preferences Initialization and Integration in Critique-Based Mobile Recommender Systems*, AIMS, Nottingham, UK, 2004.

Norman, D.A., *The Invisible Computer: Why Good Products Can Fail, the Personal Computer is So Complex, and Information Appliances Are the Solution*. Cambridge, MIT Press, 1998.

Oberquelle, H., 'Situationsbedingte und benutzerorientierte Anpaßbarkeit von Groupware', in Hartmann, A., Herrmann, T., Rohde, M., Wulf, V. (Hrsg.), *Menschengerechte Groupware - Software-ergonomische Gestaltung und partizipative Umsetzung*, Chapter of the ACM, 42, Teubner, Stuttgart, 1994, pp. 31-49.

Piper, Henning, Ohly Ansgar, *Gesetz gegen den unlauteren Wettbewerb*, Beck, Munich 2006.

Pu, P., 'User-Involved Preference Elicitation', *Proceedings of the IJCAI Workshop on Configuration*, Acapulco, 2003.

Radmacher, M., Zibuschka, J., Scherner, T., Fritsch, L., Rannenberg, K., *Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen*. WI, Karlsruhe, 2007.

Radmacher, M., 'Adaptive Customer Profiles For Context Aware Services in a Mobile Environment', in *IFIP International Federation for Information Processing*, Volume 251, Integration and Innovation Orient to E-Society Volume 1, Wang, W. (Eds), Springer, Boston, Wuhan, China, pp. 390-399, 2007a.

Radmacher, M., 'Elicitation of profile attributes by transparent communication', *ACM Recommender Systems*, Minneapolis, Minnesota, USA, pp. 199-202, 2007b,

Radmacher, Mike: A Procedure of How to conduct Research in Transparent Mobile Recommendations. In: IFIP International Federation for Information Processing, Volume 286, Towards Sustainable Society on Ubiquitous Networks, eds. Oya, M., Uda, R., Yasunobu, C., (Boston: Springer), pp. 49–60; Tokyo, Japan, 2008a.

Radmacher, Mike: Design Criteria for Transparent Mobile Event Recommendations. In: Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Toronto, Ontario, Canada, 2008b.

Resnick, P., Sami, R., 'The Influence Limiter: Provably Manipulation-Resistant Recommender Systems', *ACM Recommender Systems*, Minneapolis, Minnesota, USA, 2007, pp. 17-24.

Ricci, F., Nguyen, Q.N., 'Critique-Based Mobile Recommender Systems', *ÖGAI Journal*, Vol.24, No.4, 2004.

Ripperger, T., *Ökonomik des Vertrauens - Analyse eines Organisationsprinzips*, Mohr Siebeck Verlag Tübingen, 1998.

Sarwar, B., Karypis, G., Konstan, J. and Riedl, J., 'Item-based collaborative filtering recommendation algorithms', *Proceedings of the Tenth international conference on World Wide Web*, 2001, pp. 285-295.

Schumacher, Günter (ed.), PRIME Deliverable D1.1.d *Requirements for Privacy Enhancing Tools*, 2008, online: https://www.prime-project.eu/prime_products/reports/reqs/pub_del_D1.1.d_final.pdf

Shardanand, U., Maes, P., 'Social Information Filtering: Algorithms for Automating "Word of Mouth" ', *Conference on Human Factors in Computing Systems*, 1995.

Sinha, R., Swearingen, K., 'The role of transparency in recommender systems', *Conference on Human Factors in Computing Systems*, Minneapolis, Minnesota, USA,

Spinas, P., Troy N., Ulich E., *Leitfaden zur Einführung und Gestaltung von Arbeit mit Bildschirmsystemen*, München, 1983.

Spindler, Gerals, Schuster Fabian (eds.), *Recht der elektroischen Medien*, Beck, Munich 2008.

Swearingen, K., Sinha, R., 'Beyond Algorithms: An HCI Perspective on Recommender Systems', *SIGIR workshop on Recommender Systems*, New Orleans, LA, USA, 2001.

Sweeney, 'Latanya: k-anonymity: a model for protecting privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* 10(5), 2002, pp. 557–570

Tintarev, N., Masthoff, J., 'A Survey of Explanations in Recommender Systems', *Workshop on Recommender Systems and Intelligent User Interfaces associated with ICDE'07*, Instanbul, Turkey, 2007.

Tintarev, N., 'Explanations of Recommendations', *ACM Recommender Systems*, Minneapolis, Minnesota, USA, 2007, pp. 203-206.

Verykios, V. S., Bertino, E., Fovino, I. N., Provenza, L. P., Saygin, Y., and Theodoridis, Y., 'State-of-the-art in privacy preserving data mining', *SIGMOD Rec.* 33, 1, Mar. 2004, pp. 50-57.

Wandmacher, J., *Software-Ergonomie*, de Gruyter, Berlin, 1993.

Williamson, O. L., *Organization Theory: From Chester Barnard to the Present and Beyond*, Oxford University Press US, ISBN 0195098307, 1985.

Zibuschka, J., Fritsch, L., Radmacher, M., Scherner, T., Rannenberg, K., *Privacy-Friendly LBS: A Prototype-supported Case Study*, AMCIS, Keystone, USA August 2007.

Zipkin, P.,' The limits of mass customization', *Sloan Management Review*, 42,3, 2001, pp. 81-87.