Legal Requirements for the Personalization of Commercial Internet Applications in Europe

Schubert, Petra, Institute for Business Economics, University of Applied Sciences Basel (FHBB), Peter Merian-Strasse 86, 4002 Basel, Switzerland, petra.schubert@fhbb.ch

Kummer, Mathias, Weblaw GmbH, Laupenstrasse 1, 3008 Bern, Switzerland, mathias.kummer@weblaw.ch

Leimstoll, Uwe, Institute for Business Economics, University of Applied Sciences Basel (FHBB), Peter Merian-Strasse 86, 4002 Basel, Switzerland, uwe.leimstoll@fhbb.ch

Full reference to this article: Schubert, Petra; Kummer, Mathias; Leimstoll, Uwe: Legal Requirements for the Personalization of Commercial Internet Applications in Europe, in: *Journal of Organizational Computing and Electronic Commerce*, Vol. 16, Issue 3/4, 2006.

Abstract

Most e-commerce applications require the collection and storing of information about customers. As a consequence, the performed transactions involve legal issues. For three years, the authors have been involved in a project that studies the potentials of personalization of e-commerce systems from the particular angle of SMEs. The paper picks up a couple of scenarios that many e-commerce vendors face when implementing personalization on their Web sites. The specific focus of the discussion is the legal use of costumer profiles for e-commerce applications. Since most legal issues are difficult to understand for non-lawyers the paper makes use of a case study, which shows explicitly what e-commerce vendors need to keep in mind when implementing personalization on their Web sites.

Keywords: Legal Issues, European Law, Laws and Orders, Personalization, E-Commerce, SME, ERP

1. Introduction

The paper presents results of a longitudinal, publicly funded research project about "personalization of e-commerce applications run by SMEs". Prior project results have been presented in other publications [1, 2, 3]. In this article we will focus on an important aspect of personalization, which is often neglected by academic papers: the legal implications that arise with the use of customer profiles. Due to the ubiquitous nature of the Internet, electronic commerce does usually not stop at borders – most of its legal issues involve international legal regulations (unless the Web site explicitly excludes customers from foreign countries). The focus of our research project was on Swiss small and medium size enterprises (SMEs). For the illustration of legal aspects we chose a concrete case study in which we limited most of our discussion to the specific requirements of Swiss law with the aim of a higher degree of concreteness. However, wherever applicable we added a discussion of the corresponding European regulations. The case study shows that European and Swiss law are very similar for most questions on privacy protection with one important exception: EU law on privacy protection is only applicable to individuals whereas Swiss law on privacy protection even extents to legal entities.

Economic transactions between companies and private end consumers are subject to the law of the respective consumer. Since any international Internet retailer who does not explicitly exclude private end consumers from Switzerland is thus also acting under Swiss law, we are confident that our contribution will also be interesting for an international audience.

Personalization is always targeted at the fulfillment of a special personal requirement. It can be aimed at people as well as organizational roles in companies (e.g. a purchasing agent). Personalization in our understanding starts *after the login*. The mere speculation about a user on the basis of local cookies on the client PC that has the smack of spying on someone does not fall into the scope of our discussion. Personalization is context sensitive (regarding output for a certain user) and requires learning (by the system). The interface between the customer and the system is called "point of interaction" (POI).

For the personalization of E-Shops there are integrated software packages available, such as, e.g. One-to-One (Broadvision), Dynamo Relationship Commerce Suite (Art Technology Group), Personalization Manager (Net Perceptions) or ADAPTe (ResponseLogic), which already supply the

full range of e-commerce applications. These products are expensive and are generally destined for large companies. The standardized online shops sometimes used in SMEs only contain rudimentary tools for the personalization of transactions.

We believe that a separate consideration for these companies is meaningful because SMEs differ from corporations in many ways. In the context of the personalization of e-commerce applications the specific features of SMEs become particularly relevant. SMEs are generally characterized by limited resources and compared with corporations cannot use the benefits of economies of scale. With regard to using e-commerce applications limited financial resources, poor conceptual knowledge, lacking IT resources and low economies of scale can all have negative effects. The low economies of scale result primarily from the small size of the company because the usefulness of e-commerce applications increases with the number of transactions completed and the volume of turnover generated. In a small market segment SMEs offer specialized, high quality value products which are tailored to customers' needs (product differentiation). It is precisely for this reason that elements of personalization should also be applied in e-commerce.

Bearing in mind the established opportunities offered by personalization [4] at the beginning of the project, we had to examine the essential technical preconditions prevailing in SMEs and the general demand for personalization. These are aspects that influence the potential of personalized e-commerce applications in SMEs as well as the requirements for the development of tools for personalization.

The paper starts with the description of the research design and a literature review on personalization. The main section presents the case study of an existing SME, Tecnofil Ltd., that poses specific legal questions regarding the use of customer profiles. We summarize the findings and draw some conclusions for future research.

2. Research Design and Methodology

The research findings presented in this paper stem from a project which has been carried out since 1999 together with different SMEs in Switzerland. The reason for this project was a perceived disadvantage regarding personalization possibilities in E-Business applications, which are suitable for

SMEs compared to the possibilities of big companies. As mentioned earlier there are software packages for personalization available on the market but those systems are too expensive for SMEs. The situation is comparable to the adoption of SAP in big companies and "light-weight ERP solutions" such as Abacus or Navision in SMEs. SMEs need "easy" solutions – preferably standard software – which is cost-effective and can be customized according to the company's special purposes.

As shown in Figure 1, the project started with an empirical survey in the region. The findings were portrayed by Schubert [5]. The result encouraged the authors to proceed with the project. SMEs attribute a high value to their relationship with the customer and recognize the potential of the electronic relationship that can be supported by the operation of an e-shop. On the other hand, the survey showed that the situation for the implementation of personalization (state of know-how, existing hard and software, willingness to invest, etc.) is not very favorable in most SMEs. One important result was the need for setting a focus on the further development of existing ERP systems, which are already in use by SMEs.

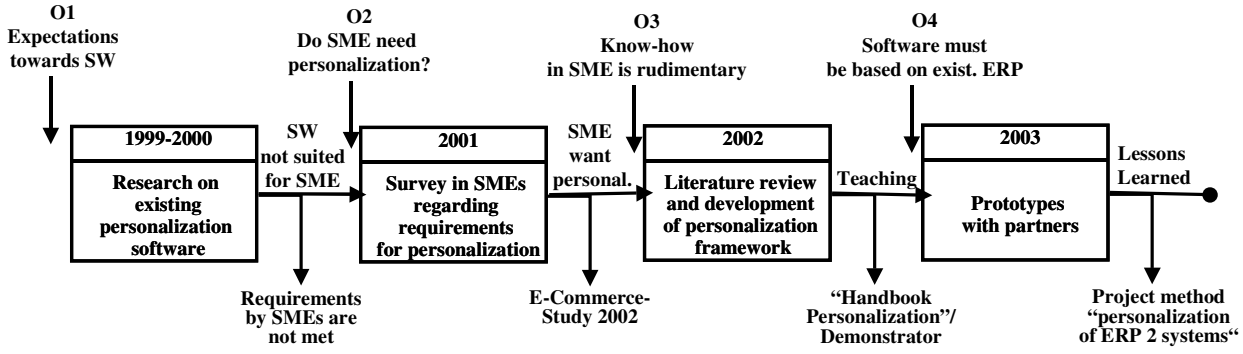

Figure 1: Steps and results of the longitudinal research project

For the illustration of the potentials of personalization we created a "handbook personalization" which shows the possibilities from a perspective, which we thought adequate for SMEs [2]. Additionally, we built a "software demonstrator" which is publicly accessible on the Internet. It displays the possibilities in a graphical form. The last objective was the development of a generic project method for the introduction of personalization of e-commerce applications on the basis of ERP systems. The project was geared at the further development of the inherently internal ERP system into a boundary-

spanning system, which integrates its peer systems run by business partners and customers. The focus of *this* paper is the discussion of legal issues, which was part of the development of the project method (last step of the project). Figure 1 shows the steps of the projects with its premises (01-04) and its milestones.

3. Literature Review on Personalization and Legal Issues

Personalization is about selecting or filtering information objects or products for a user by using information about the user account (e.g. the customer profile). The information displayed on the screen is specifically tailored according to the information already available about the user. From a technical point of view meta-information of products or information objects is matched against meta-information of users (stored in the customer profile). Personalization can be tailored to a person group or to a specific individual. In the latter case, where the information or products are customized for one single individual we speak of individualization as a special form of personalization. Personalization uses information about customers. The general term for stored customer information is "user profile" or in the context of electronic shopping "customer profile" [6].

There are various ways how e-shop operators can cultivate customer profiles e.g. "implicitly" by storing interaction with the web site (click stream) or purchase transactions or "explicitly" by asking for preferences and ratings. What formerly seemed to be possible only for the corner shop whose storekeeper knew all her clients personally, reaches a new potential in the online medium where every client leaves traces and thus "teaches" the system how to treat him differently from the other customers. This form of mass customization becomes feasible with the use of predefined rules, which can be built into e-commerce environments. These automatically personalized web sites do not achieve the high quality of corner shops but they help to establish a personal dialogue with the customer tying him or her closer to the electronic offer. Additionally, the time spent by the client to "teach" the system leads to increased switching cost. The underlying precondition is that the customer really wants to be addressed personally.

The ability to deliver personalization rests upon (1) the acquisition of a "virtual image" of the user, (2) the availability of product meta-information and (3) the availability of methods to combine the datasets in order to derive recommendations for the customer.

3.1. Systems and Concepts for Personalization

In a previous paper Schubert [3] reviewed concepts and systems that make (automatic) personalization possible in today's businesses. These driving forces can be categorized by disciplines, which are involved in personalization. The consideration of personalization ranges from a technical view in computer sciences to the economic principles of information management and marketing as far as to the global perspective of sociology. Figure 2 displays a matrix of disciplines in which personalization plays an important role. Social and information systems where personalization plays a decisive role are: virtual communities [5], social capital [7; 8], performance systems [9], CRM systems, ERP systems, and information warehouses. The respective concepts for use are: collaborative filtering [10; 11], mass customization [12], one-to-one marketing [13], CRM, permission marketing [14], viral marketing, data mining/web mining [15; 16; 17; 18]. A detailed discussion about the terms listed in Figure 2 can be found in [3]

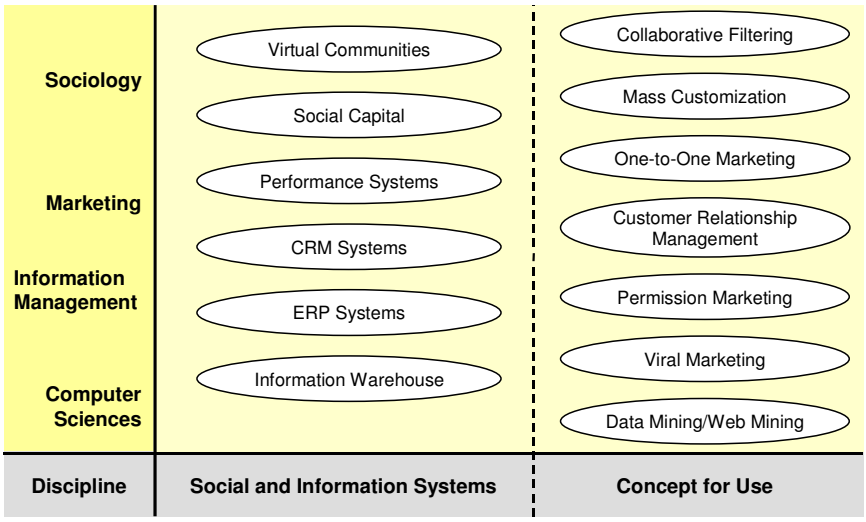

Figure 2: A multi-disciplinary view of systems and concepts in which personalization plays an important role [3]

3.2. Personalization Steps

As presented at the beginning of this chapter, one of the basic ideas of personalization is to learn something about the customers and to use this information to tailor offers for services or information to the needs of the customer. On a technical level, personalization can therefore be modeled in four steps: modeling customer profiles (requirements analysis), data input, data processing, and information output.

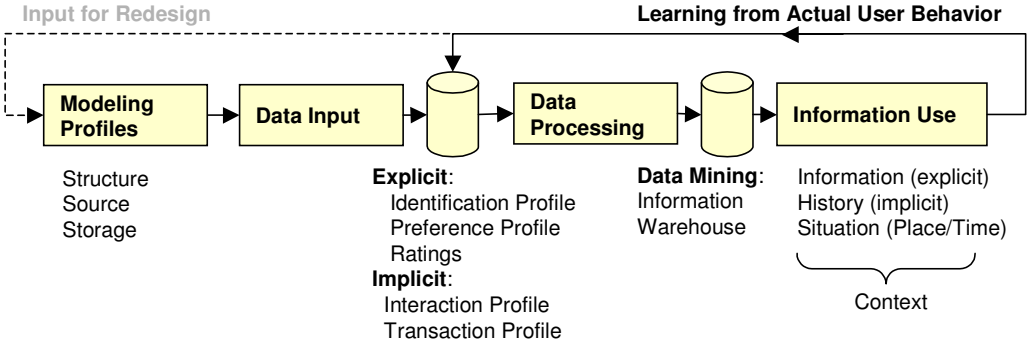

Figure 3: Customer profile life cycle [19]

In their paper „Motivating Human-Agent Interaction: Transferring Insights from Behavioral Marketing to Interface Design“ Spiekermann and Paraschiv [20] point to the fact that personalization of user interfaces depends on the intensity of the interaction with the user interfaces. The more information about preferences is available from the user the better the computer can react. The benefit that a customer can take from an e-commerce service depends largely on the readiness of the customer to actively provide information. If a customer provides false information, the recommendations derived from this data tend to be useless.

As illustrated in Figure 3, personalization is highly dependent on the professional collection and use of user profiles. The following section proposes a classification scheme for profiles. The legal use of these different kinds of profiles is examined in the case study in section 5.

3.3. Legal Issues of E-Commerce

Although the Internet has evolved into an international trading platform with no national boundaries, it is subject to national laws. So far, there are very few legal regulations in Switzerland dealing specifically with the Internet. Instead, existing law is being applied to Internet-specific facts. Companies, which operate in the Internet realm, are subject to many different laws and orders. Table 1 gives an overview of the legal areas involved and the applicable laws and orders. The abbreviations are explained in the table at the end of the references.

Legal areas	Law or Order
Rules about conclusion of a contract on the Internet, online general terms and conditions	OR
Designation of offerer, product description and declaration of price	OR, UWG, PBV
Terms of delivery, return of goods, countermand, warranty, liability	OR
Consumer protection in national and international settings (consumer law)	GestG, IPRG
Legitimacy of hyperlinks, use of third-party contents	URG, UWG, StGB
Use of domain names	MSchG, ZGB, UWG, etc.
Abidance of commercial modesty	UWG
Criminal and civil liability for contents	OR, StGB
Data protection law in e-commerce	DSG, VDSG

Table 1: List of Swiss laws and orders discussed in this paper (April 2004)

The case study of Technofil in chapter 5 contains the discussion of specific legal facts as shown in Table 1.

Whereas Switzerland does not have specific laws or regulations regarding the Internet this is different in the European Union (EU). The following table gives a summary of the most important legal areas and their contents in the EU.

Legal Areas/Contents	Laws/Directives
Harmonized regulations about • the comprehensive duty of online service providers to supply information to their users, • commercial communication, • electronic contracting, • limited responsibility of content providers.	Directive 2000/31/EG on Electronic Commerce of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of services in the information society, in particular electronic commerce in the Internal Market [21].
Increased consumer protection in modern distribution channels, e.g. Internet, e-mail, or fax. Regulation of duty to supply information and right of cancellation.	Directive 97/7/EG of the European Parliament and of the Council of May 20, 1997 on consumer protection for the conclusion of contracts in distance selling.
Effective data protection and facilitation of the exchange of personal data in the EU. • Processing of data in a legal way and in good faith • Application of the imperative of the intended purpose (no difference from the arranged, well-defined and legal purpose) • Commensurability (necessity of data collection for the intended purpose) • Securing of the correctness and up-to-dateness of the data • Deletion of identifiable data as soon as the intended purpose ceases to exist	Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [22].
Harmonization of the regulations in the different member states,	Directive 2002/58/EG of the European

which are necessary for a homogeneous protection of basic rights and fundamental freedoms. • Especially the right of privacy, with regard to the processing of personal data in the area of electronic communication. • Guaranteeing the unrestricted traffic of this data and of electronic communication devices and services in the Community. • Guidelines for the operational reliability, confidentiality of communication, communication data and processing, unsolicited mails, etc.	Parliament and of the Council of July 12, 2002 on European privacy and electronic communication.

Table 2: List of European directives regarding E-Commerce (April 2004)

However, setting up EU directives is only the first step in the European legal chain. These guidelines are binding for all member countries and have to be embedded into the respective local laws. Due to the complexity of the matter the guidelines of the EU directives are often implemented hesitantly or behind schedule by the member states. Taking Germany as an example, the above listed EU directives have particularly been incorporated into the following domestic laws:

- Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG)

  Act on the General Legal Framework for Electronic Commerce

- Teledienstegesetz (TDG)

  Act on the Utilisation of Teleservices

- Teledienstedatenschutzgesetz (TDDSG),

  Act on the Protection of Personal Data used in Teleservices

- Telekommunikationsgesetz (TKG)

  Telecommunications Act

- Telekommunikations-Datenschutzverordnung (TDSV)

  Act on Data Protection in Telecommunications

- Bundesdatenschutzgesetz (BDSG)

  Federal Data Protection Act

Further information can be found on the Web site of the German Federal Ministry of Economics and Labour [23].

The fact that the examination of Web sites must be based on the respective local law of the country where the Web site is domiciled aggravates the application of law and order in the Internet. Within the scope of this paper we will focus on a concrete case study in Switzerland. The discussion of Web sites in other European countries is likely to be similar but final legal statements can only be made after an examination of the respective local laws.

4. Customer Profiles: Where Personalization Touches Legal Aspects

The entire information about customers is usually combined in a data set called „customer profile" [24]. This data set includes all information explicitly requested from the customer and the information implicitly learned from Web activity. E-commerce systems track and store compound profiles that contain parts of the profiles shown in Table 3. Depending on the personalization methods used, there are different requirements regarding the contents and the representation of the profile.

Profile	Content
Explicit profiles	
Identification Profile	user name, role, contact information, personal browser settings, address, payment information, IP-address, etc.
Preference Profile	Self-revealed preferences (product meta-data)
Socio-economic Profile	Self-categorization in predefined classes (age, gender, hobbies, etc.)
Ratings	three types of ratings: of products, of reviews, of pages (scale e.g.: I like it – not for me)

Profile	Content
Relationships	Relationships to other users/customers (e.g. "soul sisters")
Reviews/Opinions	Plain text, images, videos and other material
Implicit profiles	
Transaction Profile	transaction log, product purchases linked to product meta-data (purchases, inquiries, payment, etc.)
Interaction Profile	click stream (pages viewed are linked to product meta-data (preference categories)
External data	Information procured from other sources (e.g. weather report, local news, events, credit rating)

Table 3: Different types of profiles [25]

As discussed above, the process of personalizing e-commerce applications involves multiple advantages for online retailers. Customer profiles can be used to display individual recommendations during the purchase transaction. Other benefits could be the reduction of marketing cost and the stimulation of long-term relationships. Internal and external cross-selling can be used to increase sales. In some cases it may even occur to online vendors to sell customer profiles – and make money with the sale. However, especially in Europe, the economic interests of online vendors are sometimes opposed to the protection of individual customer rights. Most European countries have special laws regarding data protection. The respective Swiss law is called Bundesgesetz über den Datenschutz (DSG) [26]. The general rule, which should be applied, is the following: *not everything that could be done can be done legally* [27; 28]. The EU Directives for data protection also extensively protects the privacy of people. A very good survey can be found on the EU Web page about data protection [29].

5. Case Study Tecnofil Ltd.

The following section presents the case of "Tecnofil", an existing Swiss SME, which is about to implement personalization services on its Web site. We chose this case because most of the learnings from personalization issues in this case can be applied to other companies.

Tecnofil is one of the leading producers of industrial filters in the B2B business. 25 employees produce and distribute a product range of 3'000 different air and water filters. The high product variety is a result of different filter classes, variable sizes and multiple areas of application. Most of the products are standardized. Tecnofil also offers individual products built-to-order.

Tecnofil is thinking of extending their existing Web services. The new Web site could be geared at the existing B2B customers as well as new B2C customers. The company wants to deliver extensive and current information in the area of filters. Additionally, an online order system is planned. Personalization will play an important role on the new Web site in order to facilitate comfort and increase the benefit for the customers.

The case study presents different basic scenarios and looks at them from a legal perspective [30, 26]. The first part of the analysis deals with the public area (open to "anonymous" users). The second part takes a look at the "closed user area" available for registered users only (after a previous login).

5.1. Information and Services for Anonymous Visitors (No Login)

The public part of the Web site offers information about company and services. Tecnofil has an interest in how often these pages are visited, the order of pages requested, and how often certain categories are being accessed (interaction profile). Is this kind of "anonymous log file and clickstream analysis" permissible?

Says the lawyer: The answer is dependent on the traceability back to the identity of single users. If the log file analysis is performed on the level of a specific user the activity involves issues of personal data protected by the DSG (Swiss law on the protection of personal data). Besides "safe" information such as date, time, request, and information object, log file entries usually contain the IP number of the requesting client. Without further investigation, there is no known connection between the IP number and a specific user and the log entry does thus not allow drawing a conclusion on the level of an individual user. Anonymous log file analysis is not legally problematic under the DSG [31, 32]. In the case that establishing a link between user identity and surfing behavior is possible, it has to be

conveyed to the user in the public data protection declaration on the Web site – even if the company does not make use of this possibility.

Once the company starts combining IP numbers with customer identities (after the login) the logs can be traced back to people (companies). Does it effect the legal situation if Tecnofil combines IP numbers with user accounts and starts profiling the log entries of registered users in a database?

Says the lawyer: Yes, it does. The respective person has to be informed about the purpose and the consequence of the use of the data. The database allows the link between log file data and available user data. For the use of "personal information" of this kind the consent of the user has to be obtained.

Web site visitors are given the opportunity to utter their opinion about experiences with services and products. They can make deliberate information about their person (e.g. "a contribution by Fred Flintstone from Sursee"). This contribution is afterwards made available to public Web site visitors. From a legal perspective it is interesting who is liable for incorrect statements, which lead to erroneous decisions with a lasting effect (e.g. a recommendation for the ideal change period of a filter which proves to be too long and leads to the spreading of a disease in an old people's home).

Says the lawyer: In this case we have to distinguish between civil and criminal liability. We have to also deal with the question: who is to be made liable? The author or the Web site provider?

*The **civil liability**: Potentially, people can be made liable for the deliberate provision of recommendations – as for example advice regarding the ideal period for the change of a certain filter. Advice and recommendation have to follow the requirements, which the potential reader can reasonably attribute to the information. In the case that a certain trust has been stimulated when giving the information which is worth protecting, the recommending party is liable for the adequate probability of the correctness of his/her statement (liability based on trust). Eventually, the circumstances of such a specific case would be taken into consideration.*

In our case, Tecnofil is offering a forum in which opinions and experiences from clients are being exchanged. The person giving the comment does not necessarily have to convey his/her identity. The

reasonable claim, which arises from such a statement, is not very high. A trust in the statements in an anonymous forum, which would be worth protecting, cannot be assumed. It is obvious to the visitor that Tecnofil is the provider of the forum and is not involved in the statements itself. Tecnofil is required – as far as acceptable – to delete statements, which are obviously incorrect from the forum and thus stop their distribution.

*The **criminal liability**: It is unlikely but possible that we are dealing with criminal liability in this case. In the event of criminal publications (racist information, dishonoring statements, etc.) in "media" which imply the Internet (including forums) only the author can be prosecuted. If this person cannot be determined or cannot be taken to court then the editor (the person responsible for the publication following article 27 StGB [the Swiss penal code]) can be sued. Since the statements in the forum are in an anonymous section it is conceivable that the criminal responsibility remains with the responsible person employed by Tecnofil. With this in mind it is advisable that Tecnofil does not publish information without prior examination.*

Side note 1: The question of liability of access and hosting providers for criminal content on Internet pages has been discussed quite controversially in Switzerland. Providers are considered as "helpers" if they know about the content or if the pages have been brought to their attention and have not been blocked or removed.

Side note 2: Providers should publish "rules for the appropriate behavior" (often called netiquette). Users should be told the following: "Do not write anything which you would not be willing to tell people directly. Do not pretend to be an expert. Do not misuse the forum as a marketing platform for your own purposes or for the benefit of someone else." The provider should also reserve the right to delete contributions, which are not in correspondence with the rules.

The question of liability in the Internet, in particular of host or service providers represents one of the most controversial internationally discussed questions of Online Law. The EU regulates liability of the intermediary of contents in the Directive 2000/31/EG (E-Commerce Directive, article. 12-15, c.f. Table 2). The member states are to make sure that service providers are in principle not responsible for the information which they store on behalf of one of their users. Furthermore, there should not be

a general obligation for service providers to survey the information transferred or stored or to actively search for circumstances which point to an illegal activity. Taking again Germany as an example of the implementation of this directive, the German Telecommunication Act (TDG § 11 "storing of information") states that a service provider is not obligated to survey the information transferred or stored or to actively search for circumstances which point to an illegal activity. An examination is generally not introduced until obtainment of the suspicious information.

In particular cases a liability of a provider of a discussion forum can be affirmed, e.g. if the company states in their terms that "each contribution by forum members will be manually looked at". The operator of this forum thereby self-substantiates a duty to examine and query for "highly sensitive" texts (District Court Cologne, Judgment of November 26, 2003; 28 O 706/02). Service providers should thus refrain from such statements in their terms and conditions.

Tecnofil wants to provide contents from other sources (external data). Examples are information about environmental protection or specific norms, which apply to filters. Is there anything that needs to be considered when re-publishing this kind of information?

Says the lawyer: Information from other sources which is re-published by Tecnofil on its Web site is subject to the above mentioned principles of information and advice. Tecnofil has the duty to take care and is expected to have the required expertise. It is thus reasonable to expect that Tecnofil can make sure that the information on their Web site is correct.

It has proven useful to publish a disclaimer on the Web site in which the Web site provider informs visitors that the information and opinion published on the Web site does not necessarily reflect the point of view of Tecnofil and that the author assumes full responsibility for his/her contributions. Tecnofil should also mention that they cannot grant a warranty for the completeness and the correctness of the contributions. However, the legal binding character of disclaimers is controversial [33].

It is recommendable that the information provided (e.g. about environmental norms) be annotated showing the source and the date of the online release. When re-publishing information, the provider has to examine copyright claims beforehand.

The directives of the EU reflect a similar legal situation fort his question. The judgement of external contents is depending on the knowledge of the provider. However, there has been inconsistent adjudication in the past. A compilation of German court decisions on liability for external information can be found in [34].

5.2. Information and Services for Registered Users (After a Successful Login)

The information about *existing B2B customers* is transferred and maintained in the e-shop database(s) by the Tecnofil employees. After the transfer, customer profiles are available for use by the legitimate user in the e-commerce application. The payment process is realized as beforehand: an invoice is sent by postal mail.

With the launch of the new e-shop, Tecnofil wants to grant *new customers (now also B2C)* the possibility to register themselves as customers (supplying their own customer information). Once a user logs on to the Web site, the personal information has to be completed and the *identification profile* is being stored. This includes name, delivery and invoice address, payment information (and newly also credit card information). The customer can deliberately enter preferences for product categories, for preferred means of payment, manufacturer etc. (*preference profile*). The so-conveyed preferences are being used to generate recommendations for customers regarding product categories and to facilitate the order process. Are there any measures, which Tecnofil has to take in order to store and use this personal data legally?

Says the lawyer: The described provision of data about identification and preferences are legally unproblematic. The people concerned are adding the input themselves and voluntarily. In the case of preference data users have the choice of completing the profile or not. It is important to inform new customers about the purpose of collecting personal data. New customers are to be informed in the data protection declaration that the preferences provided will be used for recommendations regarding product categories and to facilitate the order process. The personal information may only be used for these purposes (principal of restriction to purpose).

Looking at the European General Guideline for Data Protection, people concerned have the right of disclosure, access, correction, deletion and blocking for their data (c.f. Directive 97/7/EG, Table 2). These basic rights can also be found in the Swiss Data Protection Act.

Side note on data security: the law requires the use of adequate technical and organizational measures, which prevent unauthorized access to personal data. The more sensitive personal data is the better it should be protected. The collected identification and preference profiles – especially credit card information – represent sensitive data. The data has to be stored in secure databases and has to be protected from unauthorized internal as well as external access (e.g. hackers). The transfer of information should be encrypted. The protection of the system and the databases containing personal information has to be guaranteed by firewalls, adequate use of passwords and physical entry barriers.

Again looking at European Law there are several measures for data protection: Member states have to make sure that the responsible unit for the processing of data provides adequate ***technical and organizational measures*** *which are necessary for the protection of accidental or illegitimate destruction, the accidental loss, the unauthorized change, the unauthorized transfer, or the unauthorized access – in particular if data that is being transferred over a network – and against any other form of illegitimate processing of personal data. These measures must ensure, taking into account the current state of technology and the associated cost, a level of protection that is adequate for the risks involved in the processing and the nature of the data to be protected.*

The identified user (after login) has the possibility to comment on and evaluate products and services offered by Tecnofil. The Web site offers the possibility of writing opinions and experiences in specific text fields (so called reviews). The reviews are afterwards available to all visitors of the Web site. Is the publication of these reviews with the name of the author on the Tecnofil Web site permitted? Who is liable for these comments?

Says the lawyer: the liability of wrong statements has been discussed above. In the case of an identified author (linked to the user profile) the determining question in this case is the level of reasonable trust, which users have in such reviews. The danger of enforceable liability is rather

limited. If recommendations are made by acknowledge experts (filter producer, Tecnofil employees), which are recognizable, a liability is more likely to be assumed than in the case of other customers.

The customer is to be informed that his review will be published on the Web site. In the case that the name of the author is added to the review the author has to be informed (preview of page) and his/her affirmation has to be obtained. Due to the manifold possibilities of the Internet (search engines) it is easy to collect information about an individual and to use this information to compile a personality profile. This information also comprises individual contributions in discussion forums.

Apart from the already mentioned *explicit* profiles (identification profile, preference profile), which the user recognizes or even deliberately adds to the system, there are *implicit* profiles, which are being stored in the background (interaction profile, transaction profile). The users are not directly aware of their generation. Interaction profiles contain information about accessed web pages and can indirectly indicate a certain interest for product categories (meta-data). This information can be used to derive the user's interests. This also relates to data from transactions (purchases). Are there any legal implications for the storing and use of such implicit profiles?

Says the lawyer: The acquisition of such data must not be in conflict with prevailing law regarding data protection. The most important implication is that nothing should be recorded in secret. Transparency regarding the process of gathering, storing, and using personal data is required. The respective individual needs to be informed about the form of the acquisition, the purpose and the consequences. Recording of implicit data leads to a collection of data, which allows an evaluation of important aspects of the personality of an individual. Passing individual profiles to third parties without prior agreement of the individual constitutes a violation of the personality of the individual and is not permitted.

Accordingly, in European law the use of instruments such as data mining without information of the person concerned and without following the original purpose are in contrast to the protection of the informational self-determination [35].

Following article 10 of the European General Guideline for Data Protection (c.f. Directive 97/7/EG, Table 2) the person concerned is to be ***actively*** *informed about the collection of personal data. This implies in particular:*

- *The identity of the responsible person for processing the data and where applicable his/her substitute*
- *Purpose of processing for which the data is destined*
- *Recipients or categories of recipients of the data*
- *The question if the response to questions is obligatory or voluntary and possible consequences of non-compliance.*
- *Existing rights of information and disclosure regarding the data concerned provided that they are necessary under consideration of the specific circumstances which lead to the data collection to guarantee a processing in good faith for the person concerned.*

Identical or similar rights of information exist for the person concerned in the case that the data has not been collected from this person directly (article 11). The person has to be informed by the responsible person for the processing or his/her substitute at the beginning of the storing of the data or in the case of an intended transfer of data to third parties no later than at the time of the first transfer.

Germany has taken up these guidelines in the Data Protection Act (Amendment of January 14, 2003). According to German law on data protection the collection, storing and processing of personal data is now subject to permission which requires comprehensive active information about data processing.

Tecnofil wants to use the implicit profiles for the personalization of their Web site and thus to the advantage of the customer. The services based on the *transaction profile* are the following:

1. Registered users can look at the history of their past purchases (order history).
2. Registered users are supplied with product recommendations, which are calculated on the basis of anonymous sales figures from all customers.

3. All users (including anonymous visitors) are provided with anonymized reports about statistics (e.g. sales in certain product categories, regions etc.).

Says the lawyer: The possibility to look at past purchases is reasonable. The appropriate measures for ensuring confidentiality and integrity of the order history are to be taken. Product recommendations, which are based on anonymous sales figures, are not problematic. Also, the publication of anonymized reports about purchases is not problematic in general. In specific cases, e.g. where only very few and well-known customers are active in a specific region the publication of such data is not advisable since conclusions regarding their identity can be drawn.

Tecnofil analyses the *interaction profile* (clickstream) of the Web server and displays information about products, which are frequently requested by this user on the first page after the login ("your preferred products"). Customers who look at certain products repeatedly but do not buy them are being asked about the reasons in an e-mail ("help us to find the right product for you").

Says the lawyer: The user has to be informed about the above-mentioned use in the data protection declaration. Sending mail (postal mail or e-mail) to the customer is generally allowed in the case where a customer relationship has already been established. The customer has the right to request the company to stop sending such e-mails. In the event that Tecnofil keeps sending such e-mail they infringe the customer's right to preserve his/her own personality. It is also important to note that confidentiality is not guaranteed in the case of sending e-mails without using encryption. The customer has to be informed about the fact that the e-mail can be read by eavesdroppers, which gain access to the transport channel.

The EU directive 2002/58/EG on the processing of personal data and the protection of privacy in electronic communication of July 12, 2002 regulates the delivery of unsolicited mails (article 13). Commercial e-mails (spam) and other kinds of direct advertisements (fax, automatic telephone systems) may only be used with (previous) consent of the recipients (opt-in). Unsolicited commercial e-mail to people with whom a business relation has been set up previously is still permissible. Tecnofil would thus also comply with European law. In the planned scenario the customer can at any time stop the delivery of future e-mails (opt-out).

Tecnofil offers a „filter translator“ for newly acquired customers who have been using filters from competitors until now. This option is based on a table in which filters produced by competitors are linked to the “matching” Tecnofil filters which are equipped with identical technical features. The table supports customers switching from their current products to the corresponding Tecnofil products.

Says the lawyer: The translator is undoubtedly a useful instrument for the customer. Problems arise if the filter translator causes incorrect orders due to (unsuitable) recommendations. The software or the basic data could be flawed and could lead to inappropriate results. Therefore Tecnofil needs to add a disclaimer that they do not grant any warranty for the correctness of the results. If in doubt, the Tecnofil customer service team should be consulted personally by the customer before placing the order.

Another aspect connected with the filter translator is the question of unfair competition. We are dealing with unfair competition in the case that someone compares himself or his own products/services (or their prices) in an incorrect, misleading, or unnecessary degrading manner with others, their products/ services (or their prices) (following article 3 lit. e UWG [Swiss law against unfair competition]). If the filter translator does not only match filters but also displays prices offered by Tecnofil, these prices need to correspond with the current prices in the product catalog.

The Tecnofil case study was written as a reference case for companies which intent to offer personalized information based on the different customer profiles presented in Table 3 on page 12. However, we would like to point out that in most cases it will be necessary to use the professional services of a specialized lawyer to make sure that the current Web practice is not in conflict with prevailing legal regulations.

6. Conclusions and Future Research

Private consumers are the ones who are best protected by law in most legal systems. The Internet is an inherently international medium and e-commerce sites do not stop at borderlines. This means that an American Web site that also addresses a Swiss clientele (implicitly or explicitly) is subject to Swiss

law when engaging into business with the Swiss client. **Swiss (and European) law (in general) regarding data protection is much stronger than American law.** The objective is to protect the individual from information-related misuse. If American vendors do not want to be confronted with the customers' local laws [36] they are well-advised to explicitly exclude European customers from their products and services.

In this paper, we have presented results from a longitudinal research project about personalization of e-commerce systems. The different project steps have taught us that the development of personalization software is no easy undertaking. Reality shows that SMEs live in a world of heterogeneous systems – a broad bandwidth of internal systems (ERP) and different e-commerce applications (e-shop software). The operating systems in use also differ greatly. Furthermore, the majority of SMEs does not operate their own Web server, but have outsourced this task to an Internet service provider. The only possible approach was that we involved ERP solution providers, which develop standard modules for their existing software systems.

In the current phase of the project we are developing a project method for the definition of requirements for personalization of ERP-based e-commerce solutions. The project method combines a set of useful creativity tools, elements of classical project management together with a method for rapid screen design. A checklist for legal requirements containing similar questions as shown in the Tecnofil case study is also part of this project method. The most important issue is to make sure that people in SMEs and ERP vendors understand each other and manage to jointly develop a new generation of SME-suitable ERP systems, which include customizable, easy to use personalization features. Continuing with our research, we have initiated further projects with SMEs and their respective ERP vendors were we constantly apply and refine the method.

The difficulty in the development of software lies in the fact that SMEs are today cautious about the use of such systems, and the technical preconditions are not optimal due to the difference in the systems employed. Nevertheless, over the next few years, the companies which took part in our initial survey are planning substantial investments in this field [2]. After all, the study findings have

encouraged us in our assumption that a need for standardized, inexpensive personalization software for SMEs exists based on existing ERP systems, or will arise within the next few years.

References

[1] Leimstoll, Uwe; Schubert, Petra, *Personalization of E-Commerce Applications in SMEs: Conclusions of an Empirical Study (original title: „Personalisierung von E-Commerce-Applikationen in KMU: Schlussfolgerungen aus einer empirischen Untersuchung“)*, in: Weinhardt, Christof; Holtmann, Carsten (Hrsg.), *E-Commerce: Netze, Märkte, Technologien*, Heidelberg: Physica, 2002, pp. 143-158.

[2] Schubert, Petra; Leimstoll, Uwe, *Handbook Personalization of Electronic Commerce Applications (original title: “Handbuch zur Personalisierung von Electronic-Commerce-Applikationen”)*, Working Report No. 7. Basel: University of Applied Sciences Basel (FHBB), Institute for Applied Business Economics, 2002.

[3] Schubert, Petra, “Personalizing E-Commerce Applications in SMEs,” *Proceedings of the Ninth Americas Conference on Information Systems (AMCIS)*, 2003.

[4] Fischer, Rudolf; Fisseler, Dirk; Rüeger, Brian, “Five Factors Define the Success in E-Commerce” (original title: “Fünf Faktoren definieren den Erfolg im E-Commerce”), *ioManagement,* No. 12, pp. 74-79, 1999.

[5] Schubert, Petra, “The Participatory Electronic Product Catalog: Supporting Customer Collaboration in E-Commerce Applications,” *Electronic Markets Journal*, Vol. 10, No. 4, 2000.

[6] Fink, Josef; Kobsa, Alfred, “A review and analysis of commercial user modeling servers for personalization on the world wide web,” *User Modeling and User Adapted Interaction,* Vol. 10, pp. 209-249, 2000.

[7] Pennar, Karen, “The ties that lead to prosperity,” *Business Week*, December 15, 1997.

[8] Ginsburg, Mark; Weisband, Suzanne, “Social Capital and Volunteerism in Virtual Communities: The Case of the Internet Chess Club,” *Proceedings of the 35th HICSS Conference*, Hawaii, 2002.

[9] Belz, Christian, Bircher, Bruno, Büsser, Mark, Hillen, Helmut, Schlegel, Hans Jörg, Willée, Clemens, *Successful Performance Systems (original title: „Erfolgreiche Leistungssysteme“)*, Stuttgart: Schäffer Verlag für Wirtschaft und Steuern GmbH, 1991.

[10] Resnick, Paul; Varian, Hal, Recommender systems, *Communications of the Association for Computing Machinery (CACM),* Vol. 40, No. 3, March 1997, pp. 56-58.

[11] Linden, Greg; Smith, Brent; York, Jeremy, “Amazon.com Recommendations: Item-to-Item Collaborative Filtering,” *IEEE Internet Computing*, Jan-Feb 2003, pp. 76-80.

[12] Piller, Frank, *Mass Customization: A Strategic Concept for Competing in the Information Age (original title: “Mass Customization. Ein wettbewerbsstrategisches Konzept im Informationszeitalter“)*, Wiesbaden: Gabler Deutscher Universitäts-Verlag, 2001.

[13] Peppers, Don; Rogers, Martha, *Enterprise One to One: Tools for Competing in the Interactive Age*, New York: Ban-tam Doubleday Dell, 1997.

[14] Godin, Seth, *Permission Marketing: Turning Strangers into Friends and Friends into Customers*, New York: Simon & Schuster, 1999.

[15] Kimball, Ralph; Merz, Richard, *The Data Webhouse Toolkit: Building the Web-Enabled Data Warehouse*, New York: Wiley & Sons, 1996.

[16] Schweizer, Alex, *Data Mining and Data Warehousing: Orientation Aids Regarding Data Protection for Private Companies (original title: „Data Mining und Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen“)*, Zürich, 1999.

[17] Spiliopoulou, Myra, “Web Usage Mining for Web Site Evaluation”, *Communications of the ACM (CACM),* Vol. 43, No. 8, pp. 127-134, August 2000.

[18] Adomavicius, Gediminas; Tuzhilin, Alexander, “Using Data Mining Methods to Build Customer Profiles”, *IEEE Computer,* Vol. 34, No. 2, pp. 74-82, February 2001.

[19] Schubert, Petra; Koch, Michael, “The Power of Personalization: Customer Collaboration and Virtual Communities”, *Proceedings of the Eighth Americas Conference on Information Systems (AMCIS)*, 2002.

[20] Spiekermann, Sarah; Parachiv, Corina, "Motivating Human-Agent Interaction: Transferring Insights from Behavioral Marketing to Interface Design"*, Special Issue of the Journal of Research in Electronic Commerce*, 2002.

[21] European Union, *Directive 2000/31/EC - Electronic Commerce*, [http://europa.eu.int/comm/internal_market/en/ecommerce/index.htm]. [Access: 31.05.2004].

[22] European Union, *Directive 95/46/EC*, [http://europa.eu.int/comm/internal_market/privacy/law_en.htm]. [Access: 31.05.2004].

[23] Ministry of Economics and Labour, *Guideline to the Information and Communication Services Acts*, [http://www.iid.de/iukdg/english.html]. [Access: 31.05.2004].

[24] Koch, Michael; Wörndl, Wolfgang, "Community-Support and Identity Management," *Proceedings of the European Conference on Computer-Supported Cooperative Work (ECSCW2001)*, Bonn, Germany, pp. 319-338.

[25] Schubert, Petra, *Virtual Communities of Transaction in Electronic Commerce: Management, Marketing and Social Environment (original title: „Virtuelle Transaktionsgemeinschaften im Electronic Commerce: Management, Marketing und Soziale Umwelt")*, Lohmar - Köln: Josef Eul Verlag, 1999.

[26] Bund, *Systematic Collection of Swiss Law (original title: „Systematische Sammlung des Bundesrechts")*, [www.admin.ch/ch/d/sr/sr.html]. [Access: 20.06.2003].

[27] Briner, Robert G., *Contracts and Liability on the Internet: What the Manager has to Know in a Global Environment (original title: „Verträge und Haftung im Internet: Was der Praktiker im globalen Umfeld wissen muss"),* Zürich, 2002.

[28] Baeriswyl, Bruno; Rudin, Beat, *Focus Data Protection – Practice and Development in Law and Technology (original title: "Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik"),* Zürich, 2002.

[29] European Union, *Data Protection*, [http://europa.eu.int/comm/internal_market/privacy/index_en.htm]. [Access: 31.05.2004].

[30] Weber, Rolf H. (2001): *E-Commerce and Law: Legal Conditions and Electronic Forms of Business (original title: „E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen")*, Zürich, 2001.

[31] EDSB, *Data Protection and E-Commerce: Thematic Survey of the EDSB (original title: „Datenschutz und E-Commerce: Themenübersicht des EDSB")*, [www.edsb.ch/d/themen/e-commerce/index.htm]. [Access: 20.06.2003].

[32] EDSB, *Guideline for Editing Personal Data in the Private Sector (original title: „Leitfaden für die Bearbeitung von Personendaten im privaten Bereich (EDSB)")*, [www.edsb.ch/d/doku/leitfaeden/sammlungen/inhaber.pdf]. [Access: 20.06.2003].

[33] Cereghetti, Leonardo, *Disclaimer and Liability Wavers in E-Commerce (original title: „Disclaimer und Haftungsfreizeichnungen im E-Commerce"),* SIC, 2002.

[34] Feil, Thomas, Liability *for external contents, original title: „Haftung für fremde Inhalte"*, [http://www.recht-freundlich.de/download/Haftung_fuer_fremde_Inhalte.PDF]. [Access: 31.05.2004].

[35] Virtual Privacy Office, *Informational Self-Determination - What does that mean?*, [http://www.datenschutz.de/privo/recht/grundlagen/]. [Access: 31.05.2004].

[36] EU, *Data Protection Page of the European Union (original title: „Datenschutzseite der EU")*, [http://europa.eu.int/comm/internal_market/privacy/index_de.htm]. [Access: 20.06.2003].

Underlying Swiss laws:

Abbreviation	Source Law (in German language)	Explanation
OR	Obligationenrecht	Law about commerce and contracts (Commercial Code)
UWG	Bundesgesetz gegen den unlauteren Wettbewerb	Law against unfair competition
GestG	Gerichtsstandsgesetz	Law about the place and court of jurisdiction

IPRG	Bundesgesetz über das internationale Privatrecht	Civil Law
StGB	Strafgesetzbuch	Criminal Code
MSchG	Markenschutzgesetz	Protection of Trade Marks
DSG	Datenschutzgesetz	Data Protection Act
VDSG	Verordnung zum Datenschutzgesetz	By-law to Data Protection Act