Multi-dimensional-personalisation - in "whom" we trust? Perception of trust & privacy

S.W.Schilke[1,2], U.Bleimann[2], S.M.Furnell[1] and A.D.Phippen[1]

[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2] Institute of Applied Informatics Darmstadt (aida),
University of Applied Sciences Darmstadt, Germany
e-mail: steffen@schilke.net

Abstract

Multi-Dimensional-Personalisation is a new approach to offer personalisation based on dimensions like time, interest and location. This approach spans a bridge between the online and the offline world. In this paper the factor of trust and privacy in such a scenario will be discussed. In earlier papers the "Chinese Wall" was proposed as an appropriate tool for providing such privacy protection. In order to be useful and accepted the awareness of the user has to be raised to such a level that he understands that, even in the traditional offline world, there is already the danger of being exposed to a breach of privacy. Even from organisations which have a certain trust relationship to the user.

Keywords

Internet, Personalisation, Personalization, Location Based Services, Mobile Systems, Recommendation, Trust, Privacy, Chinese Wall, online, offline

1. Introduction

Multi-Dimensional-Personalization (MDP), is a personalization approach which uses several dimensions like location, interest and time (temporal component describing the "when") for the support of users in the online and offline world. Especially if these recommendations span across between the online and offline world (i.e., in a mobile environment), it requires a pro active recommendation and personalization service. Abowd and Mynatt wrote that "Most context-aware systems still do not incorporate knowledge about time, history (recent or long past), other people than the user, as well as many other pieces of information often available in our environment" (Abowd and Mynatt, 2000). The user shall be provided "… with the information they want or need, without expecting from them to ask for it explicitly" (Mulvenna et al., 2000). Besides this the content and services should be "… actively tailored to individuals based on rich knowledge about their preferences and behaviour." (Hagen et al., 1999). In the case of MDP this shall not only be based on the "surf history" but also on the history and movement patterns of the user, i.e., the location information. This is supported by Askwith which wrote that "users are concerned about the commercial misuse of their personal data for marketing (and possibly other) means. In many situations, therefore, the entire behaviour of a user may be considered private. For mobile environments we can identify four types of sensitive user information: message contents, identity, location and actions (e.g. connection to services)" (Askwith et al, 2000).

As the users are very privacy conscious such a service has to take care of providing privacy while delivering a service. Saltzer and Schroeder define the term "privacy" that it "… denotes a socially defined ability of an individual (or organization) to determine whether, when, and to whom personal (or organizational) information is to be released" (Saltzer and Schroeder, 2004). Ross Anderson describes privacy as "ability and/or right to protect our personal secrets, the ability and/or right to prevent invading our personal space" (Anderson, 2001). In the Lategan & Olivier paper (Lategan and Olivier, 2002) it was expressed that: "The privacy of information used on the Internet is a very real and important issue. Many users have concerns about the security of private information supplied to organisations on the Internet, and rightfully so, as tales of compromised information abounds.".

Privacy policies are being used more and more to promise the security of an individual's private information ..." (Lategan and Olivier, 2002). In order to achieve this the "Chinese Wall" approach is proposed which is based on a trusted middleman to allow push services based recommendation without sacrificing privacy. By doing so the organization which wants to offer recommendations can select a user group entirely based on their interests, their location and the available temporal information of the user without knowing the user personally. This way offers anonymity to the user but allows selecting a matching target audience. The vital requirement is that the user trusts the middleman (acting as the "Chinese Wall") and that the information provider is able to get his message through to potential clients.

2. In "whom" we trust

The perception of trust and privacy varies with every user and the individual experience in using online services. An interesting fact is that people have developed a distrust towards online services which has been caused by illegal activities like phising, identity theft and the suspicion that "somebody" does something with their data.

In the general perception it seems that users feel saver in the "offline" world then in the "online" world. This interesting fact has to be considered when introducing a service like Multi Dimensional Personalisation. Another interesting fact is that a study has shown that even if an internet user describes himself as privacy concerned they give out more information about themselves as they initially wanted to do (Berendt et al, 2005). So the MDP could protect users from themselves.

As this service works across the borders from the "online world" to the "offline world" it might get affected by the privacy and trust concerns of the users. As the offline world is the everyday environment in which everybody is used to live, most people do not longer see that in this world the same risks are there.

2.1. Online vs. Offline world

In the online world there will be the same or similar services available as in the offline world. By the "bad" reputation the internet has gained recently there is this "distrust" towards online transactions whereas it seems that there is a higher level of

trust towards the same transaction in the offline world. As a part of this research a survey will take place to gather more information on the perception of users. In the following paragraphs we will compare online, offline and MDP transactions a user might will experience.

As the MDP approach takes factors like the interests of the user, their location and a temporal component into account the user might think that this information could be misused.

The reality is that all these information are available in the offline world as well. If a user is using a credit card he reveals information like his interests (the purchase), the location (where the purchase took place), a monetary value (the purchase price and their account balance) and the time (when the purchase was done). All these information are available online and in real time to the credit card company. Some credit card companies constantly evaluate the transactions to protect their customers from fraud. But besides this the can also use the information for marketing purposes. Similar data is available to a bank where all the bank account data is kept. Similar to the credit card company the bank will get all the information about where, when and what a user is purchasing. Again this data can be misused as well.

To establish the link from the offline world to the online world we have a similar scenario by a mobile phone provider. Like in the other examples the mobile phone provider has a constant and real time access to the location of the user, it's movement patterns and some form of payment and interest information as well (micro payments via the mobile phone, numbers called, ring tones or wall papers).

It can be assumed that it is save to say that most users are not aware of the data which is kept in the offline world about them. All this information could potentially misused. In some form certain organisations already take advantage of this situation. The user might not be aware of it but banks and credit card companies are actively evaluating their customers based on the account balance and spending pattern. This leads to advertisements on account statements, offerings for a credit / mortgage or investment plans which are all depending on your account information.

This type of information is very similar to the data needed to provide the user with the services provided by Multi Dimensional Personalisation. If we consider this we have to convince the user that the services provided will not harm the users privacy if he would use the MDP service. In order to do so the MDP service provider has to gain the same level of trust as the traditional offline organisations mentioned above.

3. Chinese Wall approach

In various industries like banking, consulting or advertisement the Chinese Wall policy is used to keep information from one client separated from persons or teams which are working on projects or tasks or a competitor of first client. By doing so the organisation can work for two companies which are competitors and keep their confidential information separated (in theory). In the banking industry, e.g., the analysts and the investment bankers are divided by such a Chinese Wall to prevent,

e.g., insider trading. Some countries have laws in place which enforce such policies, e.g., in the financial services industries. This "non-computer" security policy attracted the interest of researchers in the security area "…, because it is a real-world information flow policy in the commercial sector rather than the usual military or government sectors." (Sandhu, 1992).

In a paper by Brewer & Nash the Chinese Wall is described that: "It can be most easily visualized as the code of practice that must be followed by a market analyst working for a financial institution providing corporate business services. Such an analyst must uphold the confidentiality of information provided to him by his firm's clients; this means he cannot advise corporations where he has insider knowledge of the plans, status or standing of a competitor. However, the analyst is free to advise corporations which are not in competition with each other, and also to draw on general market information. Many other instances of Chinese Walls are found in the financial world." (Brewer and Nash, 1989).

A Lategan & Olivier paper describes the need for the usage of a Chinese Wall in the way that: "The security of private information is of paramount importance to the continuing use of the Internet for business dealings, as the risk of fraud or unintentional disclosure of private information could be a serious deterrent to individuals. Privacy policies are being used more and more to promise the security of an individual's private information ..." (Lategan and Olivier, 2002).

Brewer & Nash explain the function of the Chinese Wall that: "We note, in the first instance, that our user has complete freedom to access anything he cares to choose. Once that initial choice has been made, however, a Chinese Wall is created for that user around that dataset and we can think of "the wrong side of this Wall" as being any dataset within the same conflict of interest class as that dataset within the Wall. Nevertheless, the user still has freedom to access any other dataset which is in a different conflict of interest class, but as soon as that choice is made, the Wall changes shape to include the new dataset. Thus we see that the Chinese Wall policy is a subtle combination of free choice and mandatory control." (Brewer and Nash, 1989). Sandhu states that: „The objective of the Chinese Wall policy is to prevent information flows which cause conflict of interest for individual consultants." (Sandhu, 1992). These are descriptions of the "traditional" usage of a Chinese Wall in industries like banking or consulting. To apply the Chinese Wall approach in a recommendation application for the Multi-Dimensional-Personalisation scenario we have to extend the traditional way of the Chinese Wall to meet the requirements.

In the Lategan & Olivier paper it was expressed that: "The privacy of information used on the Internet is a very real and important issue. Many users have concerns about the security of private information supplied to organisations on the Internet, and rightfully so, as tales of compromised information abounds." (Lategan and Olivier, 2002). Cranor (Cranor, 1999) has defined three ways to prevent that private information leaks out on the internet:

1. Private information is not disclosed at all.

2. The source of the private information is hidden, that is, anonymity is preserved.
3. Privacy policies are in effect that promise the responsible usage of private information.

By applying the first way it would not be possible to offer personalisation services at all, i.e., when the user does not trust it will be difficult to offer personalisation services as no private information will be disclosed.

As mentioned before personalisation is only possible if the user trusts at least one organisation that they will do no harm to him based on the (private) information disclosed to them. For a personalisation concept which would work with multiple sources for the recommendations a solution is to store the profile of the user anonymously (see way no. 2) with the middleman and pass a representation of this data without a real reference about the user to the participating / requesting servers. Such a type of middleman approach can act as a Chinese wall, i.e., act as in-between the user and the service provider. By doing so the organisation that wants to offer a service or recommendation to the user will only deal with an anonymous profile. This makes it necessary that the middleman follows the point 3 stated above by Cranor (Cranor, 1999).

This approach would work if there is a trusted relationship between the user and the MDP service provider (a.k.a. as the middleman or the Chinese Wall). The middleman would handle the storage, collection, maintenance and handling of the profile data of the user. In order to allow other organisations to provide recommendations or services to the users based on their profile (i.e., the combination of the interest of the user, its location and the temporal component, etc.) the middleman would take the request from the information providers and return the number of matching profiles. If the provider orders the delivery the middleman will execute the delivery of the recommendation / service offering to the users with matching profiles.

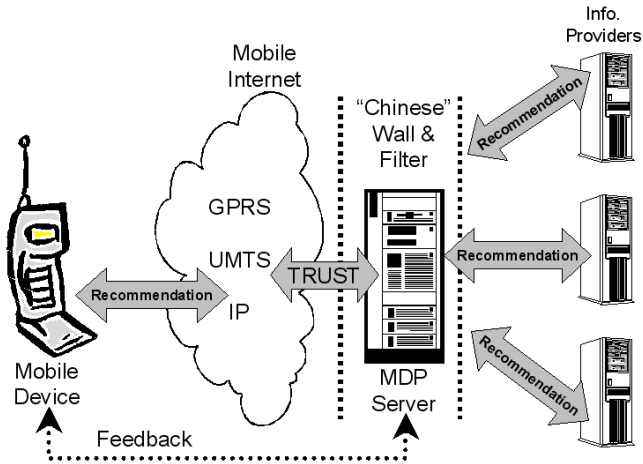

Figure 2 Multi-Tier-Architecture for Chinese Wall based recommendation

The difference between the traditional application of the Chinese Wall and the way applied in the MDP scenario is that in the traditional way a consulting company works on data of multiple clients and the teams use the Chinese Wall to prevent data from leaking from one team to the other. In the case of a middleman / MDP Chinese Wall the middleman protects the profile data of the users from the organisations which want to offer recommendations or services.

By doing so an organisation which wants to provide recommendations to MDP users would only get the possibility to select profiles which do not contain any information about the user. Kobsa expresses exactly this as a legal requirement in Germany when he writes: "User profiles are permissible only if pseudonyms are used. Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym (based on the German Teleservices Data Protection Act (1997) referenced by Kobsa (http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm #a2 – site no longer accessible)).

This clause mandates a Chinese wall between the component that receives data from identifiable users, and the user modelling component which makes generalizations about pseudonymous users and adapts hypermedia pages accordingly. Communication between these components may only take place through a trusted third component that manages the directory of pseudonyms, or through more complex pseudonymization procedures." (Kobsa, 2002).

When an organisation which wants to provide recommendations or services, it will select anonymous profiles that correspond to their chosen target audience. The middleman would take the recommendation / service offer and would pass it on, based on the selected anonymous profiles, to the "real" users. By doing so the organisation which wants to offer recommendations can select a user base entirely based on the interests, their location and the available temporal information of the user without knowing the user personally. This way offers total anonymity to the user but allows recommenders to select a matching target audience. The vital requirement is that the user trusts the middleman (acting as the Chinese Wall) and that the information provider is able to get his message through to potential clients. One drawback could be the issue of faked identities to receive, for example, discounts even if the person would normally not fit the target audience. In the application of a MDP Chinese Wall only the middleman would know if the matching profile represents a matching dog or a matching person. A user would be, for example, selected by the information in the corresponding anonymous users profile. The data in the profile would be defined by the user (e.g., the interests of the user) and the users behaviour (i.e., regular movement patterns and the temporal information collected or provided, e.g., from a schedule).

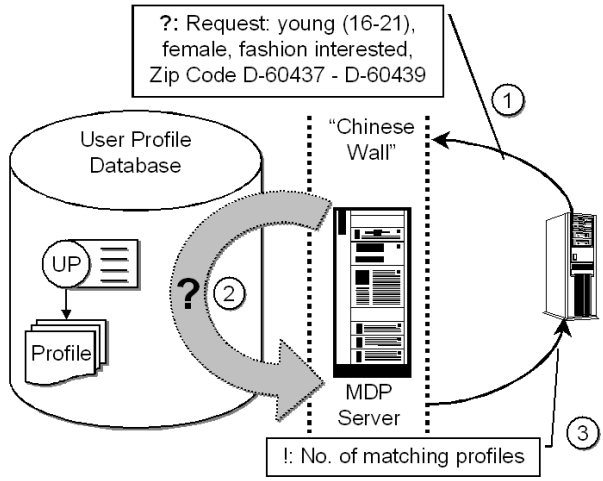

Figure 3 Request for matching profiles

Figure 2 shows that a company which wants to offer a service or recommendation to young females, aged 16 to 21, which are in the area described by the ZIP codes 60437 to 60439 (1). The MDP Service will query its database for users matching the requested profile and which are currently in the area identified by the ZIP code range (2). The service returns the number of matching profiles (3) in order to allow that the requestor can book the service.

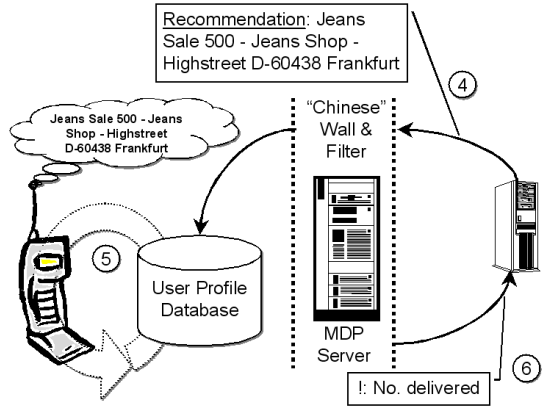

Figure 4 Recommendations are made through the Chinese Wall

An optimization for the recommendation, i.e., a "self cleaning effect" for such a system can be achieved (see figure 4) by giving the user (8) the opportunity to report unwanted recommendations (7), SPAM or even directly blocking recommendations of a certain origin (9). This will allow the MDP process to exclude this user in future requests for such a matching profile (see Figure 2 No.2) without that this information will be available to requestor of this anonymous profile.

After the requestor has booked the recommendation service (figure3, no. 4) the message is passed on to the users which fit the selection criteria (5). The requestor will be informed of the number of recommendations delivered (6). In this scenario the requestor never gets directly in touch with the user the recommendation gets send to. The user only stays in touch with the MDP provider which protects the privacy of the user by providing access only anonymous profiles to the requestor. Even if the profiles contain information about the user like their interests, their location and other information the requestor never gets "real" information about the user like their user name or phone number.

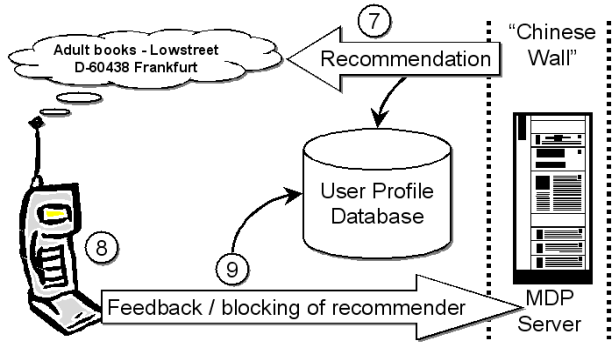

Figure 5 Feedback given for SPAM recommendation

This architecture separates the target audience, i.e., the users, from the information providers which want to reach them by using a middleman which represents the "Chinese Wall". Users have to or already "trust" somebody. As mentioned above nowadays users trust their bank, mobile phone provider or credit card company. All these organization posses, i.e., have access to sensitive data about the user which are similar to the data needed and used to provide the Multi-Dimensional-Personalization recommendations. Your bank knows how much money you have in your account and what you are spending it for and where you are spending it. The same applies for a credit card company. In the case of the mobile phone provider they also posses data about the location of the user, to whom the user is calling and which toll services (like micro payments, ring tones or images) the user is using.

This is similar to the identity protector approach which "… works in such a way as to protect the interests of the user. One of its most important functions is to convert a user's actual identity into a pseudo-identity ..." (Senicar et al, 2003). If the "... identity protector is integrated into an information system, the user may use the services or engage in transactions anonymously, thereby elevating privacy to an all-time high." (Senicar et al, 2003).

In the MDP case the user only stays in touch with the MDP provider which protects the privacy of the user by providing access only anonymous profiles to the requestor. Even if the profiles contain information about the user like their interests, their location and other information the requestor never gets "real" information about the user like their user name or phone number. Again this shows some similarities to the

identity broker approach: "When an identity protector is introduced into an information system, two domains are created: an identity domain and a pseudo domain—one in which the user's actual identity is known and accessible, and one in which it is not. The identity protector functions so as to separate the two domains and may be applied anywhere in the system where personal data can be accessed." (Senicar et al, 2003).

Even if this sounds similar to the proposed Chinese Wall the authors of (Senicar et al, 2003) suggest that the user shall control the identity protector whereas the Chinese Wall approach would act as a kind of single point of personalisation support which could be used by various applications via a common interface. This could mean that not even anonymous profiles would be made available to the requesting recommendation service, i.e. that the "recommender" would not even get access to the pseudo domain of the identity protector approach. This would even enhance the protection of the user. The MDP provider would work as "Single Point Of Trust" (SPOT) for the MDP user. I.e., the user has to trust at least the MDP provider like they do so today, e.g., as they trust their mobile phone service provider. As the MDP is clearly positioned in a mobile environment the mobile phone service provider could be the provider for such a MDP service.

SPAM, SPIM and Phishing are examples for a breach in the privacy protection of e-mail users. When the MDP service will be established this could even reach out from the online to the offline world. A MDP provider which would apply a "Chinese Wall" approach could filter the unwanted recommendations like a firewall and by doing so would add additional protection to the privacy of the user.

An optimisation for the MDP recommendations, i.e., a "self cleaning effect" for such a system could be achieved by giving the user the opportunity to report unwanted recommendations, SPAM or even directly blocking recommendations of a certain origin (see figure 4). This will allow the MDP process to exclude this user in future requests for a such a matching profile without that this information will be available to requestor of this anonymous profile. Naturally the opposite way, i.e., a subscription of recommendation from a recommendation service shall be possible.

The P3P standard (Carnor et al., 2002) could not be directly integrated into the approach as it is mainly a classification system for a web site. The standard is used to inform users on how their personal data will be used on a web site. As the mobile MDP user will only get directly in touch with a web site or services when he follows a recommendation provided. This would be the only point where the P3P standard would apply. The MDP provider site could use P3P as well for classifying their services.

4. Movement patterns

The actual movement patterns of the user, their historic movement patterns as well as calendar entries which have a location attached are vital to provide recommendations which extend from the online world to the offline world. As mentioned above the

information about the location of the user is nowadays already available to other organisations like a mobile phone provider.

Again the MDP provider will have access to this past, future and present data in order to be able to provide recommendations based on the users movement. For providing accurate recommendation the MDP provider has to analyse the movement pattern for the type of movement. I.e., if the user is walking, using a bicycle, public transportation or a car. This could be evaluated by the speed, the position of the user (e.g., street, motorway or train tracks – this depends on the accuracy of the device which delivers the position information) or by using a corresponding profile which is set by the user / device.

As mentioned above this scenario implies privacy issues as well. I.e., if the user wants to use the MDP service the user has to be aware that at least the MDP provider will know / has to know his position in order to provide the recommendation service. Again the position of the user will be only known to the MDP provider which will select the users (anonymous and matching) profile in order to provide a recommendation to the user.

5. Gathering data about and for the User

There would be several ways to gather this data. For the location and temporal information this data could be gathered automatically. For the interest dimension it would be possible to work with a controlled vocabulary / hierarchy of interests and let the user chose the matching interests.

Another, more convenient, way would be to analyse the surfing behaviour of the user to gather information about his likes and dislikes (e.g., by a rating function for sites visited or information frequently read or accessed). As Mobasher writes Personalisation should be "... done automatically based on the user's actions, the user's profile, and (possibly) the profiles of others with 'similar' profiles" (Mobasher et al, 2001).

This is where the new Multi-Dimensional-Personalisation concept can provide significant benefits to the user. This is an approach to support the user in coping with massive information overflow. The online world as well as the offline world provides a vast array of opportunities, information and services or events the might be relevant to the user. The main problem nowadays is to get the right information at the right time at the right place and in the right format.

As mentioned above a powerful extension of the model is to use a feedback function to the middleman to provide feedback about the recommendations or service offers received (similar to the ratings for Ebay™ or Amazon™ sellers/buyers). This could work in multiple ways, e.g., to block an organisation because of wrong or bad recommendations or other reasons. This feedback would allow the middleman to fine tune the service provided for the individual user. If the middleman evaluates the user feedback it would be possible to eliminate organisations which provide bad services or recommendations. If an organisation gets many bad ratings the middleman should

consider not dealing with them anymore. By doing so the service would get tailored right to the users' wishes so that everybody could receive matching recommendations and not just Spam. As positive example of this feedback approach there could be the case that a user expresses his wish to the middleman to pass more personal details to the organisation which provided a recommendation. In this case a closer relationship between the user and an organisation could be established. Naturally this relationship could be revoked if the user wishes to do so.

6. Conclusions

The need for recommendation and a guided user's experience is clear a world of information overflow. At the same time the attacks on user in the form of, e.g., SPAM or Phishing make it clear that such a service will not be successful if the user is exposed directly to the recommender. By combining the protection of the user with the possibility to offer / receive services in a "protected" fashion will make it possible for both parties to achieve their goals. The added complexity of a mobile environment will allow new services which will lead to interesting opportunities.

By using the service on the user's side and reaching the right target audience on the side of the recommender the importance of the trust relation ship to the provider of the service has not to be under estimated. A survey will be used to see how wide the gap for trusting online and offline services is, which services / applications a user could imaging using and how the service would be accepted.
An analysis of the movement patterns of the users will be undertaken. This is used to confirm if a "standard" user has "standard" movement patterns which are steady enough to be used to predict their movement so that it could be used for recommendations. In addition it has to be evaluated how future appointments from a schedule can be used to determine the future location of the user.

The proposed architecture for the Chinese Wall approach will be implemented as a prototype and tested. This design will have to tie into the whole architecture of the MDP solution. Even if the end user devices become more and more powerful a multi tier architecture shall be used, i.e., the most processing will not take place on the end users device.

By using existing standards it will be possible to implement the MDP approach on existing platforms. Missing pieces, like the constant update of location information from the end users device or the Chinese Wall service, will be implemented on top of it.

7. References

Abowd, G.D.; Mynatt, E. D., 2000: "Charting Past, Present, and Future Research in Ubiquitous Computing." In ACM Transactions on Computer-Human Interaction 7(1): 29-58

Anderson, R., 2001: Security Engineering: A Guide to Building Dependable Distributed System, Wiley Computer Publishing, New York, 2001, 612 pp.

Askwith B.; Merabti M.; Shi Q., 2000: MNPA: a mobile network privacy architecture, Computer Communications 23 (2000) 1777-1788, Elsevier

Berendt,B; Günther,O; Spiekermann,S, 2005: Privacy in E-Commerce, 2005: Stated Preferences vs. Actual Behavior, Communications of the ACM, April 2005 / Vol. 48 No. 4, 101-106, ACM Press

Brewer, D. F.; Nash, M. J, 1989: The chinese wall security policy. In Proceedings of the IEEE Symposium on Security and Privacy (Oakland, Calif., May 1-3). IEEE Computer Society Press, Los Alamitos, Calif., 206-214.

Cranor,L. F., 1999: Internet privacy. in Communications of the ACM, 42(2):29-31, February 1999.

Cranor,L; Langheinrich,M; Marchiori,M;Presler-Marshall,M; Reagle,J, 2002: W3C: Platform for Privacy Preferences, P3P 1.0, from http://www.w3.org/TR/2002/REC-P3P-20020416/ [last accessed 30.10.2004 19:34:22]

Mulvenna, M.D.; Anand, S. S.; Buchner, A.G.,2000: Personalization on the Net using Web Mining, in Communications of the ACM, August 2000/Vol. 43, No. 8, pp. 123-125

Hagen, P.R.; Manning, H.; Souza, R. , 1999: The Forrester Report. July 1999. Smart Personalization. Cambridge, MA, USA: Forrester Research, Inc., p. 8

Kobsa,A, 2002: Personalized hypermedia and international privacy In Communications of the ACM, Volume 45, Issue 5 (May 2002), SPECIAL ISSUE: The adaptive web, Pages: 64-67

Lategan,F.A.; Olivier,M.S. , 2002: A Chinese Wall approach to privacy policies for the web, in 26th Annual International Computer Software and Applications Conference (COMPSAC 2002), Oxford, UK, 940-944, IEEE

Mobasher, B.; Berendt, B.; Spiliopoulou,M. , 2001: "KDD for Personalization" in PKDD 2001 Tutorial, 5th European Conference on Principles and Practice of Knowledge Discovery in Databases September 6, 2001

Saltzer, J.H.; Schroeder, M.D., 1975: The Protection of Information in Computer Systems, http://www.cs.virginia.edu/~evans/cs551/saltzer/ [last accessed 30.10.2004 19:31:50]

Sandhu Ravi S, 1992: Lattice-Based Enforcement of Chinese Walls in Computers & Security, Volume 11, Number 8, December 1992, pages 753-763.

Senicar V.; Jerman-Blazic B.; Klobucar T., 2003: Privacy-Enhancing Technologies—approaches and development, Computer Standards & Interfaces 25 (2003) 147–158, Elsevier