Enhancing privacy through anonymous recommendation for Multi-Dimensional-Personalisation

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

[1]Network Research Group, University of Plymouth, Plymouth, UK
[2]AIDA – Institute for Applied Informatics, Hochschule Darmstadt, Darmstadt, Germany

steffen@schilke.net
sfurnell@plymouth.ac.uk
bleimann@fbi.fh-darmstadt.de
andy@jack.see.plymouth.ac.uk

Abstract: The growing availability of "Location-based Services" for mobile phones is a new target for the use of personalisation. "Location-based Services" are information, e.g., about restaurants, hotels or shopping malls with offers which are in close range / short distance to the user. The lack of acceptance for such services in the past is based on the fact that early implementations required the user to pull the information from the service provider. A more promising approach is to actively push information to the user. This information must be from interest to the user and has to reach the user at the right time and at the right place.

This raises new requirements on personalisation which will go far beyond the requirements to day. It will reach out from personalisation based only on the interest of the user. Besides the interest the enhanced personalisation has to cover the location and movement patterns, the usage and the past, present and future schedule of the user. This new personalisation paradigm has to protect the users privacy so that an approach supporting anonymous recommendations through a Chinese Wall will be described.

1 Introduction

Personalisation supports users by giving them access to information which matches their interest. It filters large amounts of information and returns a view on the information which matches the users preferences. This paper introduces a next generation personalisation approach which goes beyond the approaches of earlier personalisation projects. Besides the personalisation efforts (usually based on the users interest), the location of the user and a temporal component shall be taken into account. The approach shall enable the user and the application to span a bridge between the online and the offline world.

Abowd and Mynatt write 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" [AM00].

By adding knowledge of the future, e.g., by using information from a users schedule the Multi-Dimensional-Personalisation (MDP) approach will be able to provide even more the this. In order to provide the user with recommendations which match his interests coupled with his location and the right timing a new scheme has to be established. As there are a lot of privacy and security or trust issues involved the user as well as the provider of the recommendation has to be provided with a solution for this problem. This is supported by Askwith who 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 content, identity, location and actions (e.g. connection to services)" [AS00]. These four types of user information are sensitive because they would allow a third party to take advantage of the user, for example, by knowing the location and the identity so that the user could be tracked down. Another example is that based on the message content or the actions of the user could be misused for unwanted targeted advertisement.

2 The Multi-Dimensional-Personalisation concept

Multi-Dimensional-Personalisation (MDP) is an approach to support the user in coping with massive information overflow. There are the main dimensions: time, interest and location, and minor issues like bandwidth (e.g. data transfer via low bandwidth General Packet Radio Service (GPRS, e.g., with a download speed of 57.6 Kbit/s) or via a high bandwidth Universal Mobile Telecommunications System connection (UMTS, up to 1920 Kbit/s)), format / medium (from plain text format to rich media formats depending on the client, available bandwidth or hardware), priority (how important is an information) and cost (costs associated with information or an event). Besides these dimensions and issues there are security and trust concerns which have to be considered. The main dimensions for such a new personalisation approach are:

- the time dimension: comparable to a calendar or schedule. The user has a certain repeating behaviour (always in a similar time frame, e.g., the way to / from work, lunchtime, etc.) or schedules some trips ahead. The MDP would build up on this information and would allow a permission based recommendation taking into account the interest of the user and the location of the user. This would allow to recommend future events as well as events which fit the regular schedule of the user;

- the location dimension: taking the movement pattern of the user into account. Regardless of whether the user is using a desktop PC, a notebook, a mobile device like a PDA or smart phone, he will always be "somewhere". Either at home, at work or on the road there always will be interesting things or information related to this user. Combined with the other dimensions it is possible to offer recommendations "just in time" at the right place. Even planning ahead in time would be possible. Reoccurring moving patterns of a user can be tracked and used for recommendation based on the users location;

- the interest dimension: (termed “personalisation” in prior approaches) addresses what the user is interested in. This can range from business or commercial interests which are related to the job or studies to private interests like hobbies. These interests can be grouped in profiles to allow switching and prioritising between them.

The minor issues which have been mentioned above can be taken care of during the implementation of the system. For example, issues like bandwidth of the communication, technical capabilities of the device used to participate, etc. For example the bandwidth issues would limit the amount of information which could be sent to the users device. The service would have to limit the amount of information transferred from a rich media message down to text messages depending on the available bandwidth.

It seems that in existing systems, and in previous work or literature, such an MDP approach has not been taken before. There are usually the two main dimensions in existing personalisation systems - interest and location. The interest based personalisation usually uses filtering techniques like content filtering, collaborative filtering, rule based filtering, content mining, monitoring of the surf behaviour or by selection of interest topics through the user for the personalisation or recommendation to the user. For the location-based services or personalisation information request, a pull style implementation is usually the standard approach in current systems (for example, the user has arrived at a certain location and has to request the information he wants). Furthermore, some systems nowadays deliver / push information to a client if a certain program (e.g., routing / navigation) is started or a certain services is requested.

These methods have to be extended to be applied in the Multi-Dimensional-Personalisation context and have to be taken into account for the proof-of-concept or implementation phase. The user shall be provided "… with the information they want or need, without expecting from them to ask for it explicitly" [MU00]. Besides this the content and services should be “… actively tailored to individuals based on rich knowledge about their preferences and behaviour." [HA99]. Nielsen writes on his web site that the "… bottom line is that for enabling Smart Personalization techniques the application needs to recognize individuals, not computers" [NI02]. By taking this into account and considering that personalisation usually happens only on one web site or within a portal (e.g., in an intranet) the requirements should be clear. This new approach proposes services which will provide the user with the possibility to use his profile across all participating web sites. As Schafer et al. writes “One classification of delivery methods is pull, push, and passive” [SC01]. In order provide good services for the user it shall be an interactive solution providing the result of the Multi-Dimensional-Personalisation in form of a proactive push to the user. This requirement was described, e.g., in [CH98] that "an optimal assistant provides the required information autonomously and independently, without requiring the user to ask for it explicitly". The user shall get "… the right information at the right time and place - with minimal interaction" [CH98].

As mentioned before the location-based services approach is nowadays generally used for mobile devices like mobiles or smart phones. In such scenarios the information is generally used to navigate the user to a service or information provider. This is connected to a certain need or demand of the user (e.g., a pizza restaurant, a hotel or such things). This is mainly an "on demand" scenario, i.e., the user requests / pulls the information and has to select "what" he wants. The location-based personalisation provides the "where" information for the "what". A literature search has not found a system proposed which really combines these two dimensions in a personalisation engine. At present, there is no approach known to the authors that combines the third dimension, time, with the two other main dimensions. Another issue is that there are no real approaches known that try to bridge personalisation between the online and the offline world.

2.1 Recommendation for the Multi-Dimensional-Personalisation scenario

There is a specific trust and privacy issue for the recommendation part as there are data protection laws in place which can cause problems for such a function. Besides that the users are very conscious about their privacy when they are using a service. The wish to stay anonymous or having their privacy protected is vital for the success of such a system. These functions can only be successful if the user trust the entity which provides this service and passes on the recommendations. Similar trust relationships already exit to organisation like banks, mobile phone companies or credit card companies. This seems odd at the beginning but if we consider that all these organisations have information about their customers and their behaviour, their location when using the services provided and a kind of knowledge about their interest (e.g., from their shopping pattern (bank & credit card companies) or mobile phone companies (e.g., numbers called or services requested and paid for). Nowadays these organisation do not directly provide any real form of personalisation or location-based services. The only way this existing data about the users is used is, e.g., when a credit card company is analysing the "normal" behaviour of a credit card customer to identify "abnormal" behaviour, i.e., usage of the credit card to prevent fraud. This analysis of the behaviour is usually based on the usage location as well as on purchasing patterns.

2.2 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 phishing, 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 [BE05]. 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 be 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 apply.

2.3 Online versus Offline worlds

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.

A way to achieve this trust by the user is to put the right protection of the private data in place. An implementation of a Chinese Wall is a way to implement such a barrier which protects the privacy and anonymity.

3 The 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." [SA92].

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." [BN89]

Lategan & Olivier describe 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 ..." [LO02].

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." [BN89]. Sandhu states that: „The objective of the Chinese Wall policy is to prevent information flows which cause conflict of interest for individual consultants."[SA92]. 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.” [LO02]. Cranor [CR99] 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 [CR99].

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.

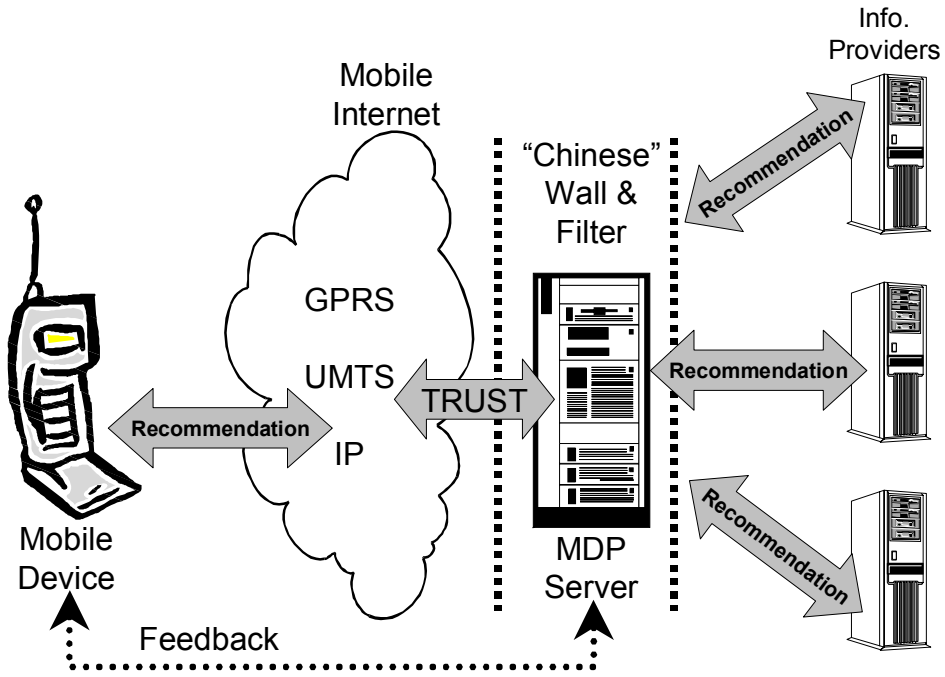

Figure 1 Multi-Tier-Architecture for Chinese Wall based recommendation

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[1]. 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." [KO02]

[1] Based on the German Teleservices Data Protection Act (1997) reference by Kobsa (http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm#a2)

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).

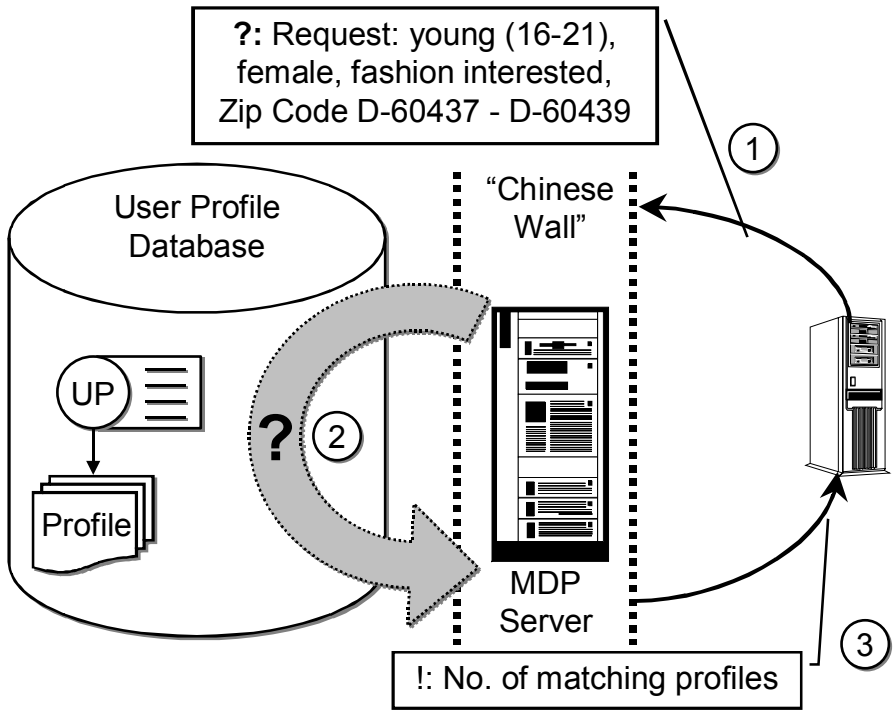

Figure 2 Request for matching profiles

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.

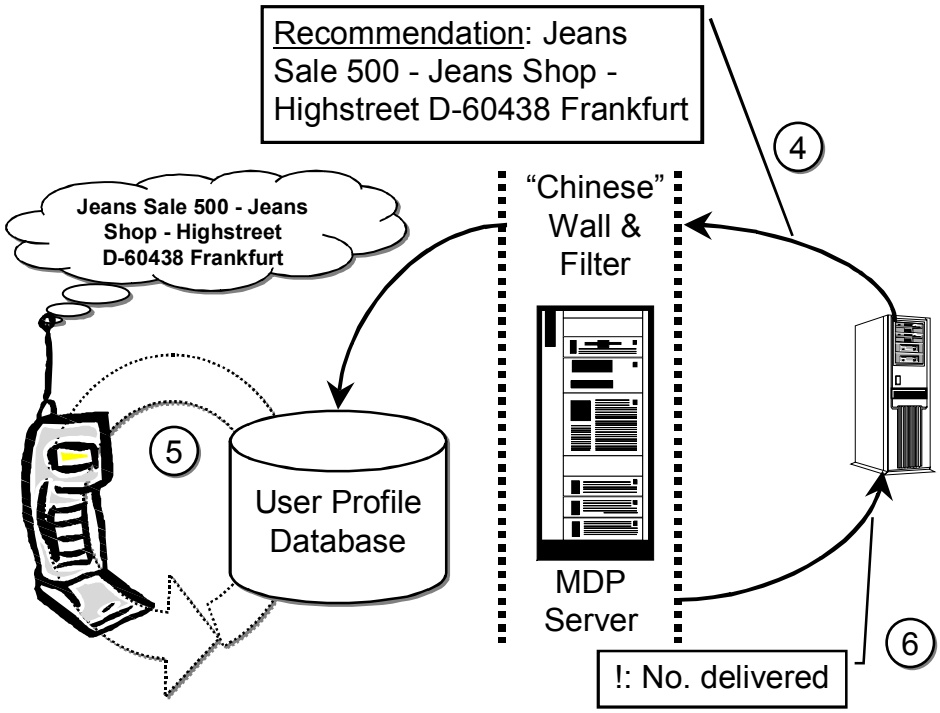

Figure 3

Recommendations are made through the Chinese Wall

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.

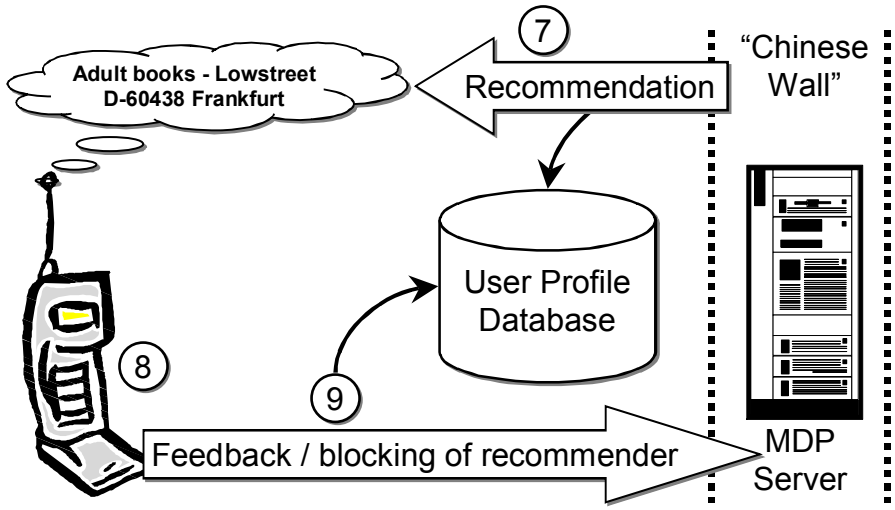

Figure 4 Feedback given for SPAM recommendation

An optimization for the recommendation, i.e., a "self cleaning effect" for such a system can be achieved 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 a such a matching profile (see Figure 2 No.2) without that this information will be available to requestor of this anonymous profile.

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 and by doing so would protect the privacy of the user.

3.1 Trust, privacy and the Chinese Wall approach

This architecture separates the target audience (i.e., the users) from the information providers that want to reach them by using a middleman which represents the Chinese Wall. Users already have a "trust" relationship to somebody. 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 ..." [SE03]. This part is similar to the Chinese Wall approach. Both protect the users identity and profile so that the "... user may use the services or engage in transactions anonymously, thereby elevating privacy to an all-time high." [SE03].

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."[SE03]. The main difference is that the Chinese Wall is the "Single Point Of Trust" (SPOT) for the user and can act as a privacy hub for many applications freeing the user from having to take care of its protection for every single application.

Even if this sounds similar to the proposed Chinese Wall the authors of [SE03] suggest that the user shall control the identity protector whereas the Chinese Wall approach would act as a kind of single point of personalization 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 SPOT for the MDP user. The user would have to trust at least the MDP provider like they, for example, 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 optimization 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. This will allow the MDP process to exclude this user in future requests for such a matching profile without that this information will be available to requestor of this anonymous profile. Naturally the opposite way, namely a subscription of recommendation from a recommendation service, shall be possible.

The P3P standard [W302] 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.

3.2 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.

3.3 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" [MO01].

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 to deal 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 an 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.

4 Conclusion and Research Outlook

The Chinese Wall has been described as a potential scenario for a trust and privacy platform for Multi-Dimensional-Personalisation. The main issue for its deployment is that the MDP service provider has to win the trust of the users. As shown users already have trust relationships to several organizations like banks, credit card companies and mobile phone service providers. The main point is to keep this trust relationship and extend it to the new type of service.

For the implementation a design decision has to be made on how to implement an automatic matching of either profiles or chosen interests. One approach is to apply, e.g., an adapted vector space model based algorithm which identifies matching profiles by comparing the vectors of the user profiles and the offerings (similar as the vector space model is used to cluster documents). The mapping of the past, actual and future location of the user and their interests as well as temporal component like estimating when the user will be where. The temporal component will be based on the past, present and future schedule of the user, his movement patterns / behavior of the past which will be know by the MDP provider. As the devices used by the mobile users are usually smart phones most of the processing has to be done on a server hence the Multi-Tier-Architecture which uses the smart phone only as thin client.

For the communication between the middleman and the user standard protocols could be utilised. But still the architecture has to be designed to support the mobile users of the future. For the interfaces which accepts the recommendations a web service based architecture is advisable.

One approach is to get to know the potential users of the MDP approach better by an online survey. This 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.

There has to be an analysis of the movement patterns of the users. It has to be confirmed if a standard user has movement patterns which are steady enough to be used to predict their movement so that it could be used for recommendations. This will be undertaken by using a GPS data logger and some volunteers. In addition it has to be evaluated how future appointments from a schedule can be used to determine the future location of the user. This could be achieved by extending calendar formats with an location component. This could cover the final location as well as trip data if available.

The proposed architecture for the Chinese Wall approach has to be implemented as a prototype and field 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.

5 References

[AM00] Abowd, G.D.; Mynatt, E. D.: "Charting Past, Present, and Future Research in Ubiquitous Computing." In ACM Transactions on Computer-Human Interaction 7(1): 29-58, 2000

[AS00] B. Askwith et al., MNPA: a mobile network privacy architecture, Computer Communications 23 (2000) 1777-1788, Elsevier

[BE05] Berendt et al., Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM, April 2005 / Vol. 48 No. 4, 101-106, ACM Press

[BN89] Brewer, D. F.; Nash, M. J: 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. 1989.

[CH98] Chavez, E.; Ide,R; Kirste,T.: SAMoA: An experimental platform for Situation-Aware Mobile Assistance. in Proceedings of Workshop on Interactive Applications of Mobile Computing 1998

[CR99] Cranor,L. F.: Internet privacy. in Communications of the ACM, 42(2):29-31, February 1999.

[FO90] Foley, J., van Dam, A., Feiner, S., Hughes, J.: "Computer Graphics, Principles and Practice" second edition, Addison-Wesley, Reading, MA, 1990

[HA99] Hagen, P.R.; Manning, H.; Souza, R.: The Forrester Report. July 1999. Smart Personalization. Cambridge, MA, USA: Forrester Research, Inc., p. 8, 1999

[KO02] Kobsa,A: Personalized hypermedia and international privacy In Communications of the ACM, Volume 45, Issue 5 (May 2002), SPECIAL ISSUE: The adaptive web, Pages: 64-67, 2002

[LO02] Lategan,F.A.; Olivier,M.S.: 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, 2002

[MO01] Mobasher, B.; Berendt, B.; Spiliopoulou,M.: "KDD for Personalization" in PKDD 2001 Tutorial, 5th European Conference on Principles and Practice of Knowledge Discovery in Databases September 6, 2001

[MU00] Mulvenna, M.D.; Anand, S. S.; Buchner, A.G.: Personalization on the Net using Web Mining, in Communications of the ACM, August 2000/Vol. 43, No. 8, pp. 123-125

[NI02] Nielsen, J.: Supporting Multiple-Location Users. Jakob Nielsen's Alertbox, at <http://www.useit.com/alertbox/20020526.html>, May 26, 2002

[SA92] Sandhu Ravi S: Lattice-Based Enforcement of Chinese Walls in Computers & Security, Volume 11, Number 8, December 1992, pages 753-763.

[SE03] V. Senicar et al., Privacy-Enhancing Technologies—approaches and development, Computer Standards & Interfaces 25 (2003) 147–158, Elsevier

[SC01] Schafer, J. B.;Konstan, J.A.;Riedl, J: E-commerce recommendation applications, Data Mining and Knowledge Discovery, 5(1-2): 115-153, 2001

[W302] W3C, Platform for Privacy Preferences, P3P 1.0, 2002 from www.w3c.org