Towards Privacy-enhanced Mobile Communities – Architecture, Concepts and User Trials

Markus Tschersich[a,*], Christian Kahl[a], Stephan Heim[a], Stephen Crane[b], Katja Böttcher[a], Ioannis Krontiris[a], Kai Rannenberg[a]

[a]*Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security, Grüneburgplatz 1, 60629 Frankfurt am Main, Germany*
[b]*Hewlett-Packard Labs, Long Down Avenue, Stoke Gifford, BRISTOL BS34 8QZ UK*

Abstract

With the advent of mobile broadband technologies and capable mobile devices, social communities become a ubiquitous environment for people to stay in contact and share information with friends and fellows. This provides new opportunities for communities and their providers (e.g. regarding advertising) but also implies new question regarding the privacy and trust of their users. We argue that a balance needs to be found between these (partially) diverging interests and motivate, why a new approach to identity management and users privacy is necessary in this context. Based on requirements retrieved by real-life communities, we describe an architecture including privacy enhancing concepts and advanced privacy respecting advertising, which addresses such requirements. We further describe the architectures' prototypical implementation, and present for the first time evaluation results based on user trials with two different mobile communities.

Keywords: Mobile Communities, Privacy, Trust, Identity Management, Targeted Advertising

1. Introduction

The emergence of localisation-capable (e.g. based on GPS, Wi-Fi, etc.) mobile devices, the advent of the Web 2.0 paradigm, and the introduction of 3G broadband wireless services created the right conditions for a new ecosystem of services that allow the extension of virtual communities (social networks) to the mobile paradigm. Within this paradigm people connect and form communities via their mobile phones and allow users participating in their community wherever and whenever they want.

A mobile community is based on a group of people generally united by shared interests, but the set up of the interaction is supported by mobile communication technologies. Compared to typical web-based virtual communities, the new technological possibilities introduced new aspects in mobile communities. Interactions between the community members became more spontaneous, enabled by the anytime-anyplace connectivity of their mobile devices. Furthermore, location information was introduced in the exchanged content, based either on GPS in the devices or other localization methods in mobile networks. This enabled not only new types of content that are bound with location, but also new ways to distribute content or create new bonds (e.g. who is around me, etc.).

This new setting created new usage patterns from the users and combined with the fact that mobile phones are so tightly coupled with our personal sphere, sharing information through them raise privacy concerns, including the fact that people might be leaving private information traces they are not even aware of. This increased public awareness of privacy and several research studies present convincing data that such concerns have an impact on people's acceptability and adoption of these new technologies.

However, communities are made to share information among users and also service delivery often requires information about the individual, either to tailor the service or simply to deliver the product. Consequently, communities are now, and will continue to be, challenged when trying to cope with the conflicting demands of managing personal information and protecting privacy. On one hand, personal information is required to build a successful community, and on the other hand,

[*] Corresponding author
Email address: markus.tschersich@m-chair.net (Markus Tschersich)

it is a source of potential damage, if not properly managed. This imposes a need for ICT services to support the community and utilize identity management functions. It also raises the following questions for participants:

- Whom can I trust with my identity and other personal information?
- How is identity information and personal information handled, i.e., stored where, accessed and/or processed by whom and for what purpose, transferred to whom for what purpose, etc.?
- How is content that I share with the community handled?

Personal information of users is desirable not only for service provisioning, but also for enabling business models based on marketing and advertising. For the communities themselves, marketing and advertising means a possibility to generate revenues and to finance their services, while from an advertiser's point of view, communities represent an ideal place for personalized marketing and targeted advertising. However, as shown by several marketing related activities by online communities, users are not always willing to share their personal information for marketing purposes.

The aspect of privacy in communities becomes even more relevant for advertisers as well as for users, when these communities make use of context information that is available in a mobile usage context. In particular, location information may be used in mobile communities for location based community services (e.g. friend finders). Location information means further opportunities for advertisers, because advertisements and other marketing activities could be presented to a user not only based on his or her user profile, but also based on current context. On the other hand, the fact that, besides the characteristics of a user, information about his or her location is also available makes the question of who has access to this information more important. The area of conflict between the need for privacy of individual community users on one hand, and the opportunities of personalized marketing on the other, demonstrates the relevance of privacy issues for communities, especially in the mobile usage context.

In fact, a balance between the involved parties (User, Advertisers and Community Provider) has to be found, as all of their interests matter to a certain degree. That does not necessarily mean that it is a fixed balance between privacy and marketing. The mentioned mechanisms of identity management can give users the opportunity to specify a particular degree of privacy, and show that the importance of privacy for the users is recognized.

1.1. Stakeholders

Around a community service, several stakeholders are placed with different interests and ambitions. On one side there are stakeholders, interested in the community service as a pool of potential customers and information about them. On the other side there are stakeholders interested in the service itself and personal advantages.

As shown in Figure 1, a central role is played by the Community Service providers. They provide a set of services to well-targeted communities. Such services include information publishing and sharing, community oriented communication services, and the creation of direct connections between members.

Community operators operate the community services. Normally, they give the community service their brand and act as the contact point of that community. In many cases the community operator and the community service provider is the same organisation. But it is also possible to have both as separate organisations.

Third-parties are offering additional services for a community service. This could be commercial and advertising services, but also other services like games, databases, etc. The third-parties are in communication with the community service provider and the community operator. Third-parties have a contractual relationship with the operator and they have to coordinate the technical interfaces with the service provider in order to integrate their services into the platform.

By joining online communities and participating through the sharing of information and user generated content, community members help the online community to develop and grow. They hence become an attractive target for advertisers, and help generate more money for developing the community service.

Finally, Mobile and Convergent Operators deliver the basic communication services that are key elements to supporting communication services within the communities (voice communication, messaging, mail, multimedia).

1.2. Contribution

The goal of this work is to present a new approach to identity management, for enhancing trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks. In particular we address the trust, privacy ad identity issues in new, context-rich

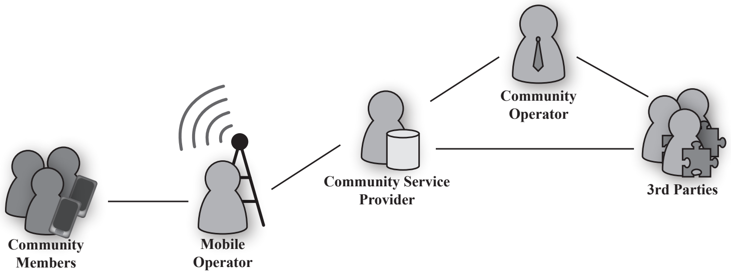


Figure 1: Overview of the stakeholders implicated in provisioning of services in mobile communities.

mobile communication services, especially community-supporting services. Additionally, we try to describe how information flow and privacy requirements can be balanced in complex distributed service architectures also in combination with third-party application like advertisers etc. We try to highlight how theses issues can be solved in an acceptable, trustworthy, open and scalable manner.

As a first step to address these questions, our approach is to analyse related contemporary research. Following that, we gather requirements from privacy sensitive communities in a bottom-up approach. Further we present a community platform architecture including concepts to address the gathered requirements and enable open, privacy-respecting identity and trust management. In the research project PICOS[1] these architecture and concepts were prototypically implemented in a community platform and community applications, and they were tested in user trials. This is the first time that such privacy concepts have been tested in practice and this paper communicates their evaluation and the experiences we gathered from real-life mobile communities.

More specifically, the paper is organized as follows. Section 3 focuses on the process of gathering requirements andSection 4 presents the overall architecture, where the requirements have been transformed into adequate concepts and features for communities. In Section 5 we describe the implementation of these concepts as features in the aforementioned community platform and the first community applications. In Section 6 we elaborate on the findings from the user trials and the lessons learnt. Finally, Section 7 concludes the paper and discussed future research challenges.

2. Related Work

Online, social and mobile communities are well present in current research. Probably, this is caused by the popularity of nowadays communities like Facebook, Myspace or Loopt. Various aspects on (mobile) social networks and privacy and trust are discussed intensively in literature, e.g. by (Chew et al., 2008; Adu-Oppong et al., 2008; Hiltz and Passerini, 2007; Preibusch et al., 2007). Usually the focus is on online social networks (OSNs), not considering the special aspects of mobile communities, where the context (e.g. location) is continuously changing, making it much harder for users to control privacy, compared to the relative static situation of OSNs.

Particular issues of mobile communities are discussed e.g. in (Görlach, 2004), where a study on concerns in social communities is presented, and in (Sadeh et al., 2009), which includes privacy, trust and security aspects in the context of location-based services. Such works also partially contain some proposed solutions, like e.g. privacy policies and concepts to control location disclosure. The work by Görlach (2004) is also focused on improving privacy awareness, by giving users feedback on their behaviour. In a way, work has also been done by various research projects such as PRIME[2] , PrimeLife[3], PEPERS[4] and DAIDALOS[5]. However, the work within these projects was merely focused on different aspects. E.g., PRIME focused on privacy-respecting identity management, but not in the context of (mobile) social networks, while PrimeLife is working on privacy in communities, but not with regard to a specific application domain. PEPERS researched a mobile peer-to-peer security infrastructure with the

[1] www.picos-project.eu

[2] www.prime-project.eu

[3] www.primelife.eu

[4] www.pepers.org

[5] www.ist-daidalos.org

focus on decentralised trust and identity management, considering individual stakeholders (e.g., journalists) and centrally managed employees, instead of communities. Also DAIDALOS concentrates on the single user and not on communities with regard to privacy-friendly ubiquitous services.

Regarding work in relation to the advertising approach, there are a few publications that focus on aspects of marketing and advertising with regard to social networks. While some rather focus on general aspects, such as business models (Hoegg et al., 2006; Palmer, 2009), many focus on the application of viral marketing in the context of communities (Leskovec et al., May 2007; Kempe et al., 2003; Hartline et al.; Subramani and Rajagopalan, 2003). Kahl and Albers (2010) are concerned with a deeper integration of marketing into the communication processes within social networks and provide the basis for the advertising concept described in this paper.

Hence, there is little significant work which addresses the focus of PICOS, to enhance identity management in mobile community services in order to consider the diverging needs of stakeholders, as described in the introduction of this paper.

3. Requirements

Social, online or mobile communities are built on communication flows and relationships between their users. Therefore, it is important to become aware about users' preferences and needs before starting to research on how to enhancing privacy and trust in communities. Especially in the field of mobile communities with additional information about users' location, there is a gap between the privacy needs that are considered important by the literature and the privacy needs desired by the users themselves (Barkhuus and Dey, 2003). The involvement of users in the development life-cycle can help to focus on their real needs and plays an important role for the success of ICT systems (Clavedetscher, 1998). Especially at the very early stages of a project, developers can benefit from involving end users to acquire and consolidate requirements and domain knowledge effectively (Rumbaugh, 1994; Holzblatt and Beyer, 1995). Based on that, to gather user requirements in the field of trust, privacy and Identity Management (IdM) in mobile communities is essential to investigate on concepts how support community users in these fields.

Users have to deal directly, as well as indirectly, with privacy and trust questions in the domain of communities, which may raise their awareness in this domain. This further contributes to empowering users to handle and manage the disclosure of their personal data and the protection of their privacy, not only on a technical level but also with respect to conscious awareness. In addition, it is expected that a system designed considering the advice of specific selected group of end users, will find broader adaptability by the respective communities.

Nowadays social communities differ regarding their needs for trust, privacy and IdM. With respect to their structures, stakeholders' intentions, objectives and mobility, privacy, trust and IdM needs vary between different categories of communities. Covering users' needs for all categories of communities is hard to realise. Thus, focusing on exemplary communities helps us to narrow the scope and to clearly define the problem space. Therefore, we selected three exemplary communities to accompany the development of privacy-enhancing IdM solutions for community services: *recreational anglers*, *independent taxi drivers* and *online gamers*.

Each of these exemplary communities benefits from mobile community services and shares a general need for trust, privacy and IdM. Despite these similar needs, those three groups differ by their characteristics, purposes and goals, and the specific requirements of their stakeholders, as described in (Liesebach and Scherner, 2008). Recreational anglers, for example, are organised in various kinds of communities, e.g., angling clubs/associations, or networks of loose friends. The members of these real world communities interact in various ways, e.g., they arrange meetings, prepare angling trips, share information (e.g., pictures) about their last angling trip with friends, or just inform themselves on weather or environmental information when they are angling (Arlinghaus et al., 2002). Within such community interactions they share more or less private information, wherefore they have an inherent need for privacy and trust.

In close connections to representatives of the three selected and focused communities, we have identified community-specific as well as general requirements with respect to trust, privacy and identity management. Stakeholders were interviewed individually to understand their attitudes and needs regarding trust, privacy, and identity management in the light of next generation community services. The complex feedback given by these community stakeholders has been categorised, explained, and backed by rationales for the stakeholders' vital interest that the requirements they stated become addressed. These community-specific requirements are mainly based upon interviews with community experts and representatives, questionnaires and observations. As a result of this work, 48 requirements have been gathered to address trust, privacy and identity management aspects that are significant in the particular domain.

Type	Requirement
Trust	Personal Trust
Privacy	Data Minimization
	Confidentiality
	Definition of Privacy Settings
	Visibility and Reachability
	Unlinkability
	Fine-grained Disclosure and Sharing of Data and Information
Identity Management	Partial Identities
	Subsequent Release of Identity Attributes

Table 1: Selected requirements.

In what follows, we give more details for a subset of requirements, also listed in Table 1. Those requirements are selected, because they are most relevant to the presented concepts in the following sections.

Personal Trust. People are familiar with personal relationships and they tend to establish trust primarily based on these well-known procedures as they adhere also to personal expectations. This requirement transfers the support of building trust based on personal relationships, functional relationships, group identification and reputation to the digital world.

Data Minimisation. In many cases, users are not aware which kind of data is sufficient to be able to use a certain service. As a result, they are easily persuaded by service providers asking for more information than what is actually needed. By providing guidance to users on what is an appropriate amount of personal information that they should provide to others, the system helps users to understand their options and to link their own actions of providing information to the context they are acting in. Furthermore, the system therewith supports the users' right to be informed before the processing of data starts and allows rectifying, erasing, or blocking their data.

Confidentiality. Users want their personal information only accessible to selected groups or users. Data protection of personal information requires special mechanism to ensure data is not disclosed to unauthorised individuals/systems.

Definition of Privacy Settings. The community has to ensure that community users are able to define suitable privacy settings regarding their preferences, needs and related to their context. Experiences made with existing approaches and systems let users want communities to provide flexible and easy-to-use system to set their privacy on a granular level.

Visibility and Reachability of Users. Users want to decide in a context-dependent way, how, when, where, and by whom they want to be visible. The community platform has to ensure that appropriate support is provided to users to help them define their visibility levels towards others.

Unlinkability. Unlinkability is required for community users to interact with certain stakeholders in specific contexts without the opportunity to link all their single activities to one identity. However, in some cases interactions within the community may call for a certain kind of linkability, e.g., contacting users in the context of data ownership.

Fine-grained Disclosure and Sharing of Data and Information. Users want to have the opportunity to manage the disclosure, the sharing of their personal data and user-generated content on a fine-grained level. Special attention has to be paid to location information to enable selective sharing of location data with others.

Partial Identities. The system must support users in grouping personal information, location information and other attributes to different (partial) identities and to act under them according the current context. For each partial identity they can selectively decide which personal information of their real identity is also part of this partial identity. The same individuals can have different roles/profiles in the same or different communities.

Subsequent Release of Identity Attributes. Users do not want to reveal all attributes of their identity to a partial identity at once. Additionally, users also do not want to publish identity attribute always to all communication partners. Users want to be empowered to control the assignment and disclosure of their attributes that are part of their partial identity while considering the current context and keeping user's privacy and confidentiality.

4. Architecture

The PICOS community platform architecture represents a technical framework which aims to integrate enhanced concepts of privacy and identity management within community related functionalities. The architecture has been designed to satisfy the needs of several stakeholders, as described in Section 3, and in parallel minimise the tensions around privacy. In Section 4.1, we describe the concepts around which the architecture is build, in order to address these requirements. Then, in Section 4.2, we will see the technical components that realise these concepts.

4.1. Concepts

The elaborated concepts address the gathered requirements described in Section 3. They aim to provide users with tools that help them managing the disclosure of their personal information in multilateral interaction scenarios. The concepts can be subsumed under four different categories:

- Enhanced Identity Management,
- User Controlled Information Flows,
- Privacy Awareness Support, and
- Advanced Targeted Advertising.

An exemplary subset of the architectural concepts is listed in Table2, together with the requirements they address.

4.1.1. Enhanced Identity Management

Based on the concept of mobile identity management (Müller and Wohlgemuth, 2005), the PICOS architecture supports users in managing the disclosure of their current position and mobile identity in communities. The concept of Partial Identities (pIds) (Hansen et al., 2004) in particular allows users to create diverse identities with different sets of personal attributes (such as name, age, preferences) for various contexts and purposes. By means of pIds, users can have several identities within one community, as shown in Figure 2. Then they decide for each identity which personal information they want to disclose in every interaction. Each pId appears to other users of the community as a unique, individual member with its own profile. The profile information is based on the so-called root profile, which is only visible to the user. It contains all information provided by a user. The profile of a pId is derived from this root profile and comprises a subset of its information. The relation between the different pIds is only visible to the user and the community operator. Only one particular pId can be active at a certain time. The user is able to switch between pIds while acting within the community by choosing the most appropriate one for the respective situation.

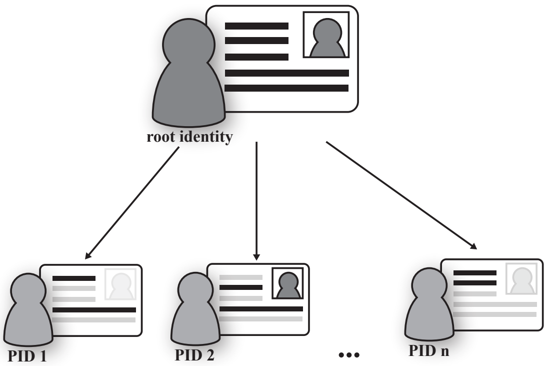


Figure 2: Partial Identities.

For instance, if a user participates in different subcommunities, Partial Identities allow him to reflect different aspects of his personality within these subcommunities and to hide or reveal relationships between different elements of his personal information.

4.1.2. User-controlled Information Flows

As our gathered requirements show, a balance is needed between publishing personal information to use functionalities of the community and keeping a certain degree of privacy (Liesebach and Scherner, 2008). Hence, several of our concepts support users in maintaining their privacy while still being able to use the community and its features as they want.

In mobile environments, location information is of specific interest, e.g., for location based services (LBS). Such services are also of interest to mobile communities, since they allow e.g., friends to be displayed on a map or information to be shared about interesting spots in close vicinity. The interest in a user's location for services like Gowalla , Foursquare and Facebook Places is increasing, in particular, if users are encouraged to visit particular locations (e.g. a specific caf) and share this information with their friends within the community. However, usually there is only the option to either show or hide completely one's own position, e.g., as implemented in the previously mentioned Loopt service. The advanced concept of *Location Blurring* gives users

PICOS Concept	Addressed Requirements
Enhanced Identity Management	
Partial Identities	Personal Trust Unlinkability Partial Identities Subsequent Release of Identity Attributes
User Controlled Information Flows	
Location Blurring	Definition of Privacy Settings Visibility and Reachability of Users Fine-grained Disclosure and Sharing of Data and Information
Private Site	Confidentiality Definition of Privacy Settings Fine-grained Disclosure and Sharing of Data and Information
Privacy Awareness Support	
Privacy Advisor	Data Minimisation

Table 2: Selected requirements and corresponding concepts.

the additional ability to hide their exact position without being completely invisible to others. It foresees the obfuscation ("blurring") of a user's current position or a point of interest at various degrees (Figure 3).

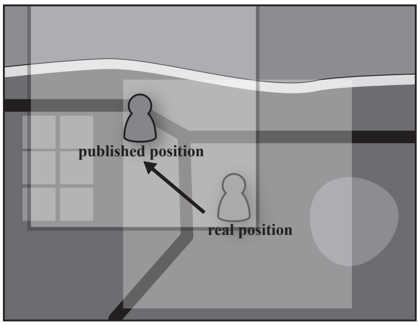


Figure 3: Location blurring.

Blurring can thereby also be used at certain places where users do not want to be localised exactly or at certain times. In combination with additional privacy policies users are allowed to specify, which other users are able to see their exact position and their blurred position. The policies allow to define in fine-grained detail, and for each of a user's pId, which information is available to other users in a defined situation (e.g., with regard to location information).

Besides blurring, the concept of *Private Sites* provides also location information within the community. A private site remarks a private area, defined by location coordinates, radius parameter, title and site description, as shown in Figure 4. This could e.g, be a user's home or working place. With regard to such a site the end-user is able to attach privacy rules in order to state who (which contacts) will be authorized to see his location information when he is close that private site. Thereby blurring and privacy policies can be used to blur or hide the position location-based, within sensitive private areas like one's home.

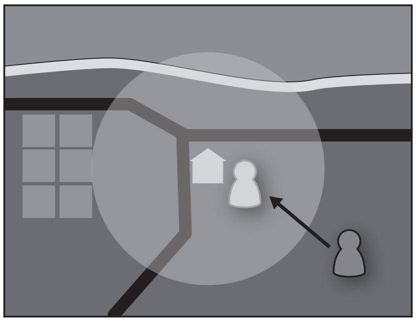


Figure 4: Private site.

The Policy Manager supports the user in attaching privacy rules to the private sites. Once the private site is defined, users can use the Policy Manager and attach a privacy rule to the created site (for instance, that the location of the user should be visible to specified other users, if the user is close to this private site with a certain distance).

4.1.3. Privacy Awareness Support

Managing privacy by means of pIds and Privacy Policies may become a complex task. The Privacy Advisor is designed to provide guidance on privacy related matters that may affect members as they interact with the community. It serves as a guide which provides hints and additional information, when it comes to privacy relevant actions of users (e.g., provision of personal information in a user profile). However, privacy (and trust) is subjective, and it is often difficult to find a single "right answer" to questions and concerns about privacy. Hence, the Privacy Advisor is context sensitive and provides hints in specific situations when personal information of users is involved (e.g., disclosure of location information, registration and profile management). It warns a user when disclosure of information might place the user's privacy at risk. One challenge in this context is to understand what information a member values most in a given context. The Privacy Advisor operates in real-time, looking for evidence of activities that may undermine the member's attempt to remain private, and by alerting the member regarding actions that may expose sensitive personal information.

4.1.4. Advanced Targeted Advertising

Advertising is an important mean for social network providers to generate revenues, and it is hence an integral part of many providers' business models. Consequently, in order to finance or co-finance social networking services, the infrastructure often needs to be open for marketing activities of sponsors/advertisers (Hoegg et al., 2006). Social networks are especially attractive for targeted advertising, as their users provide detailed personal information. However, a balance needs to be achieved between the needs of users for a privacy respecting usage of their data and their interest in relevant advertising information, as well as the interests of the advertisers and finally those of the social network provider (Liesebach and Scherner, 2008).

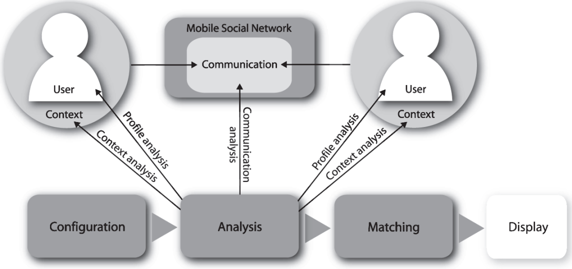


Figure 5: The advertising concept: Direct and indirect support of communication processes.

The Advanced Targeted Advertising concept enables targeted advertising activities under consideration of context information and users' privacy preferences. Based on previous research (Kahl and Albers, 2010), we aimed to provide the opportunity to enable targeted advertising, considering extended user information, while giving users control about the use of their personal information.

Based on the idea to integrate advertising into the context of the communication processes within social networks (Palmer, 2009), advertisers can directly provide targeted communication (targeted ads) to social network users (Business-to-Consumer communication (B2C)), based on profile and context information. Users, who match with the target profile to a defined degree, are provided with the advertisement. For the targeting, profile information, as well as context and communication information of users is considered.

In addition, as shown in Figure 5, advertisers can indirectly support the communication between users and thereby support viral marketing processes (Consumer-to-Consumer communication (C2C)) (Kotler and Armstrong, 2006). They can create a target profile in order to identify "key users", which should be addressed in order to further spread the advertisement. These users are regarded as opinion leaders, which have a stronger influence on their social surrounding (Dobele et al., 2005; Phelps et al., 2004). Depending on the actual advertisement which shall be delivered, there are different definitions of who the "key users" are. For example, these can be users, who are very active with regard to communication or users who have many relationships to other users (friends) or certain characteristics (e.g., a certain age).

By supporting direct communication between advertisers and users as well as supporting interactions between users, the benefits of targeted advertisements (Nielsen, 2009; Ho and Kwok, 2002; Beales, 2010) are enriched with the advantages of viral marketing activities, based on the intensive social interactions between users. The communication between advertisers and users becomes more tailored to the individual user and is in consequence presumably more relevant. The users are further encouraged share the advertised contents with other users who have similar interests (Schulz et al., 2007; Dobele et al., 2005).

In both cases the social network provider acts as an intermediary between these two parties. This is a key element as it ensures that personal data of users is neither given to third parties nor that third parties have any direct access to it. It further ensures that the previously described privacy enhancing concepts can be applied by the provider with regard to advertising (e.g Privacy Policies). The social network provider serves both the advertisers and the users/consumers, while respecting their specific interests (e.g., privacy of users). In addition the advertising concept considers privacy preferences of users and enables users to control the information which may be used for advertising.

4.2. High-Level view on the architecture

The architecture is based on a client-server topology. The clients (e.g., smart phones) can process local services but can also rely on the community for shared services. Additionally, the host can also take the service in the case that it is too demanding in terms of computing and storing resources. Communities that wish to interact with each other, an external advertising agency, or a specialist service provider, are interconnected at the services level. Managing the complex and challenging issue of inter-community trust is the responsibility of the community operator, who acts on behalf of members.

4.2.1. Components of the architecture

Based on the client-server topology the architecture comprises several technical components. Figure 6 shows a high-level view on the architecture. This view highlights the key features, namely user management on the left-hand side and service provision on the right hand side. In the following these components are described in more detail.

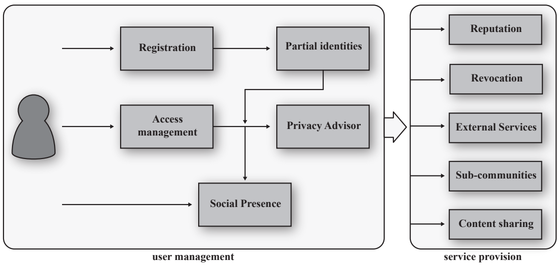


Figure 6: High-level view of the PICOS architecture.

Registration management The registration component (Figure 7) handles the registration of an individual to acquire him the membership of a community and to get access to the community and its resources and services which are only accessible to members. During the registration process the registration component calls the Partial Identities management component to generate a unique root identity for each new member. Additionally to the root identity, a first pId related to the root identity is created to enable the new member to interact in the community. At this point of time the new member also provides personal information that he is generally willing to share in his root identity. This personal information is collected and saved by the profile management.

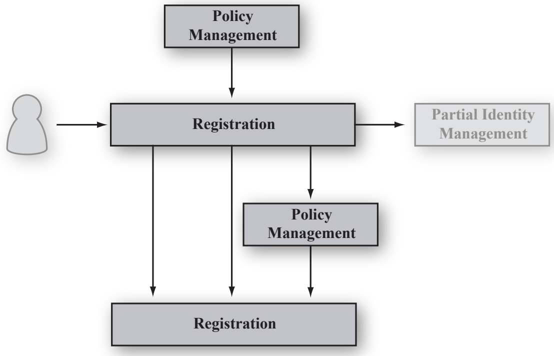


Figure 7: The Registration component.

Partial Identities management Responsible for managing the different partial identities of a community member and its root identity is the Partial Identities management component (Figure 8). This component enables the member to create, change and delete all his pIds. But at least one partial identity is required for every user. The Partial Identity management is in close connection to the profile management to handle the personal information of a member and to enable him to match his personal information attributes with one or more pIds.

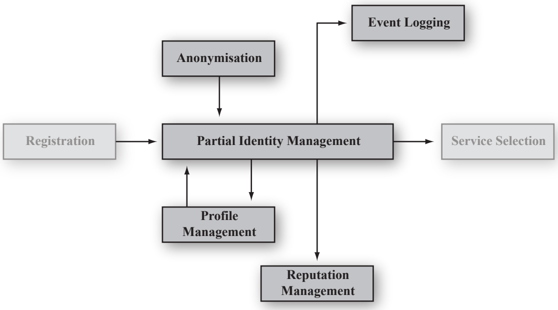


Figure 8: The Partial Identity Management component.

Access management The access management component acts as a gatekeeper by controlling access to all community resources. This combines authentication and authorisation functionality, which are both provided as separate Tier-2 components. Additionally, this component handles the access of guests and third-parties. On receipt of a request to access the community, the access management gathers indication and authentication information for validation. In the case of a successful authentication, access to the community is granted.

The access management component also sends the information about the login of a member to the social presence component. This component enables to publish member's presence and location to the community based on his privacy settings.

Privacy Advisor The privacy advisor component is responsible for informing a user about potential privacy risks, when he acts within the community. The specific role of the Privacy Advisor includes: Enhanced Content Monitoring, Community Dynamics, Workflow Awareness, Policy Matching, and Social Presence.

Enhanced content monitoring. Includes the scanning of user generated content for personal information, when the content is shared with sub-group members or shared publicly. Scanning involves 1) content tags (e.g., name, description, etc.) and 2) the body of the content contributed (where the body is interpretable), and applies to situations where 1) a member is about to intentionally disclosed information that is personal and sensitive, and 2) is about to accidentally or unintentionally disclose information. The examination involves the matching of the above mentioned tags and body with 1) previously defined personal information stated in the member's profile, and 2) predictable information (e.g., email address, credit card number, telephone number).

If the user is sending sensitive information, e.g. as defined in the User's Profile, it will send a notification to the user warning him of the risks. The user reacts by deciding whether he wants to send the information anyway, or cancel the sending.

Community Dynamics awareness. The Privacy Advisor component may be activated for a variety of reasons, e.g. by the Service Selection component, External Service Delivery component and Scenario Management component. This means that the Privacy Advisor will check/scan posted threads, in the same way as asynchronous message content.

Workflow awareness. The architecture and the Privacy Advisor in particular, considers the full life-cycle of membership activity, from registration with the community, interaction with other members, use of shared facilities, and ultimately concerns that arise when a member terminates membership of a community but leaves personal artefacts behind.

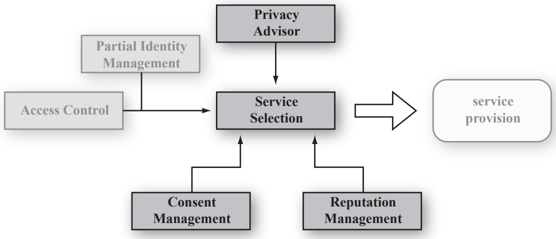


Figure 9: The Service Selection component.

Privacy Policy Matching The Privacy Advisor performs Privacy Policy matching when as member joins a sub-community, where the Privacy Advisor will check the member's own privacy policy rules against the rules of the sub-community or the sub-community creator/owner (assuming that the sub-community inherits the privacy rules of the creator). It compares the privacy rules of the member, just prior to them joining the sub-community, with the privacy rules of the sub-community. An exception results in a notification being sent to the joining member. The Privacy Advisor automatically selects the exception detection mode, where exceptions are defined as 1) a difference in values (e.g. only interact with female members vs. a male member), or 2) an out-of-bounds variation (e.g. only interact with member of neutral or positive reputation vs. member with negative reputation).

Social Presence The Privacy Advisor notifies the member if they publicly revealed their position in high-risk settings (locations), and suggests suitable remediation, i.e., turn off or blur/increase blurring. Detection situations include: 1) A member is notified if another member, who is not a trusted member of their sub-communities, attempts to access their location. 2) A member moves unintentionally and leaves location blurring off as they move to a new location, having previously turned blurring on to assist nearby members.

Social presence The social presence component controls the visibility of a member to other members in the community. This component enables members to express their reachability and willingness to share current status information. It accepts, stores, and distributes social presence information to other members who are interested. The social presence of a member is only available to the current active partial identity.

Additionally, this component manages the visibility of the location of the members currently used location. In correspondence with the Partial Identity management and the anonymisation component the social presence component also realise the blurring and private site concept.

Reputation The reputation component is used to provide an indication of the trustworthiness of an entity. This entity is typically a member of the community. Reputation is an important mechanism for building trust between community members, and forms the basis for making recommendations. The reputation component handles the reputation received from members and calculates users reputation to be published in the community.

Revocation The revocation component manages the process when a member wants to leave the community. Revocation will trigger to make the data of the member who wants to leave the community anonymous if it is not possible to delete all data because of discussions or entries in the community. It is also the task of this component to handle data of a partial identity when it will be deleted.

External services The task of the external service component (Figure 10) is to ensure that external services are delivered according to the level and quality of service previously defined and agreed with the community operator and members. Additionally, this component controls how members access external services and limits the amount of the used members' personal information. Another task of this component is to control the delivery of content and notifications from the service provider to community members by using the content sharing component.

A special part of external services is the above mentioned advertising. As we will see in Section 4.2.2, it provides an interface to external advertisers, which enables them to conduct different advertising activities on the platform.

Sub-communities The sub-community component is responsible for managing sub-communities created by Partial Identities. This component's task is to manage how the different partial identities of a member interact with external- and sub-communities. The sub-communities' role is also to integrate external- or sub-communities into a member's profile and to maintain a list of members who can access to those communities by using the profile management.

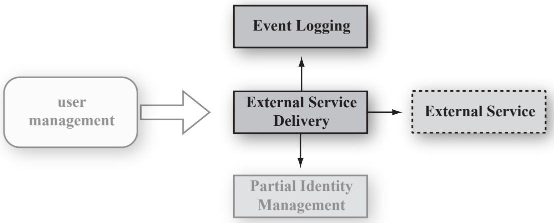


Figure 10: The External Service component.

Content sharing The task of the content sharing component is to manage to publish content to be available for single or a group of the members of the community. This component contributes, administers, manipulates and communicates content imported by one member to the community. By doing this the content sharing component also manages the import and export of content elements (e.g. by uploading photos etc.). This component works together with the Partial Identity component because to guarantee that every content element is related to a partial identity.

4.2.2. Advertising Components

The advertising component consists of two sub-components, which support B2C communication and C2C communication, as described in Section 4.1.4. Both sub-components integrate the privacy policy management. They only target users which have not generally disabled advertisements and they consider only the attributes a user has approved to be used for advertising.

Support of B2C communication. The sub-component enables the configuration of advertisements (content, form) and target profiles for advertisers. The form of an advertisement can be a selection of different types, e.g., banners, pop-up, message, invitations to brand specific groups. By defining the attributes of the target profile, the advertiser can describe those users which he wants to target. This can comprise all attributes a user provided by the users' profile (e.g., gender and age), context and communication activities, but also context based attributes like the current distance to the advertiser's shop and communication activities (e.g., forum contributions). The more precise this definition is, the more accurate could individual users be targeted. The gathered information leads to a dynamic user profile, which contains the profile, the context and communication information about the user.

In addition, the advertiser can configure, how many attributes need to be equal, in order to achieve a "matching" of target profile and user profile. For each attribute the advertiser can also configure if this attribute needs to match in any case. In this case no matching can be achieved if these "necessary" attributes are not fulfilled.

Support of C2C communication. The sub-component enables the configuration of advertisements (content, form) and target profiles of the key users. The configuration resembles the process for B2C communication support including the specification of the target attributes. As only a limited number of matching users should be addressed, these key users are the users which match best with the target profile.

To support the action of forwarding (spreading) of the delivered message, advertisements contain a possibility to immediately and easily share them with other users (e.g. "forward" button). This simplifies recommendations and it supports existing intrinsic motivations of users to forward advertised messages (Pousttchi et al., 2008).

5. Development and Testing

Based on the architecture described in Section 4, the PICOS research project implemented two community prototypes and a platform prototype. During the project the prototypes were intensively tested in user trials with end users of two exemplary communities, an angler and a gamer community. In this section we give more details about the development of the community prototypes and explain how the trials were performed, before we present the evaluation results in Section 6.

5.1. Prototype Development Process

The PICOS prototypes were developed in a two cycle's approach, spanning over a period of three years. In cycle one, a community prototype for an angling community has been developed, consisting of a platform prototype and a client prototype. In the second cycle, the angling prototype was enhanced and in addition the prototype for the gaming community was developed. The implemented prototypes are based on a duplex Remote Procedure Call (RPC) model. The platform is defined as a web service interface, with an embedded RPC gateway, based on HP technology. The client accesses the platform using a RPC, with a client RPC library provided in the handsets J2ME environment. Regarding the platform each component acts as a web service server. The requests are decoded by PHP SOAP libraries and methods are called by the PHP SOAP server (Caradec, 2010).

The Anglers Client prototype and the Gamer Client prototype use a Nokia 5800 as a hardware platform and the J2ME (Java 2 Mobile Edition) environment. The Gamer application communicates via https with the RPC Gateway and via http with a third party map service. The external interfaces of the second platform prototype have been defined using the WDSL language, describing the platform interface in a single WSDL document. Therefore it is possible to build client applications also on other hardware platforms, e.g., based on Android or other mobile OS.

Originally, 49 components were identified in the architecture to describe a privacy-enhanced system, spanning the client, the platform and the environment in which they are deployed. A subset of components was selected, to be included in the prototypes. The objective of the selection was to choose generic components that are community-agnostic and that help to address the key PICOS themes of identity, privacy and trust management for community applications (e.g. the Privacy Advisor, Partial Identities component or the Subcommunities component). The selection was based on an analysis of nine previously developed use cases, describing common user scenarios in mobile communities. To demonstrate the community agnosticism, the two developed community applications work in front of the same platform prototype.

5.2. Implementation of selected concepts

The architecture of the community prototypes are built around two central concepts, the object model and the policy model. The platform is defined as a set of objects with attributes and children objects. There are two root objects which are the user object and the public community object. The user object is the root element for any attribute that is user related. The public-community object is the root element for any object that describes the overall community besides the member of the community. The policy engine is in charge of storing rules attached to various objects or attribute of objects as well as evaluate user actions based on the set of rules.

It is typically a generic rule engine that embeds intelligence to evaluate rules and deliver a response (status) on the required action. Whenever a component of the community prototype performs an action on an object, it has to ask the policy manager to evaluate. It is the caller component responsibility to enforce the response sent back by the policy manager component.

5.2.1. Partial Identities

For the PICOS platform, user and pIds are different objects with a pId object owning only a sub-set of the user attributes. pId automatically inherits from user object the attributes that are generic to the user (e.g., location, some user profile attributes, etc.). However, attributes like location that are not redefined at the pId level can still be accessible using a pId. A user profile is associated to an identity and contains sensitive static user information thus excluding privacy rules, reputation, presence or location. The primary identity profile contains the full definition of the user information. The partial Id profile can only redefine a sub-set of the profile attributes. As an example, the gender of the user is defined at the primary identity profile level and all partial identities attached to that user will see the same gender without being able to modify it on a per pId profile level.

Creating a partial identity also creates a specific context for the user-profile, the presence, the privacy rules and the reputation. These identities are used to reference the user in any operation in the public community. Identities are externally known through the notion of pseudonyms, which is the only mandatory field of the profile to complete.

5.2.2. Privacy Advisor

The Privacy Advisor (PA) is implemented as a special assistant embedded in the platform whose role is to inform the end user of non-obvious possible consequences of his actions on his privacy (personal information is revealed). Technically, a PA instance is attached to each registered user. Some of the Privacy Advisor interactions with the end user are just notifications; others require the end user to acknowledge the consequences of the request, before the request is taken into account (i.e., confirm publication of content detected to contain personal information). For example, the PA scans the information appearing in profile attributes like *family name*, *location*, *street name*, *phone number*, *zip code*, *email*, *Skype-ID* or *Facebook*. These attributes are checked inside the following content types:

- Category content (in the file description, and inside a plain text file)

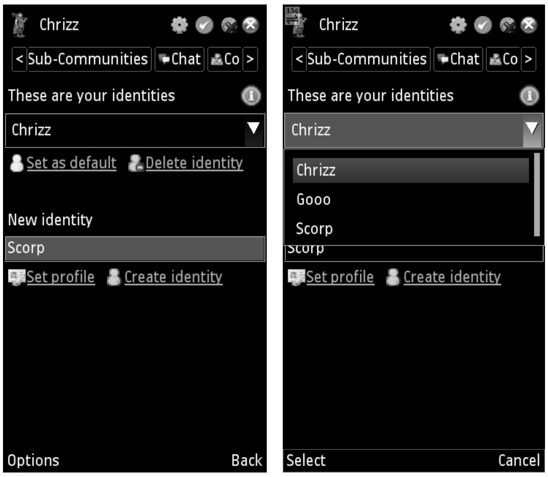


Figure 11: Creation and switching of partial identities.

- Forum-thread contributions, and inside a plain text file attached to the post.
- Chat messages
- Asynchronous messages

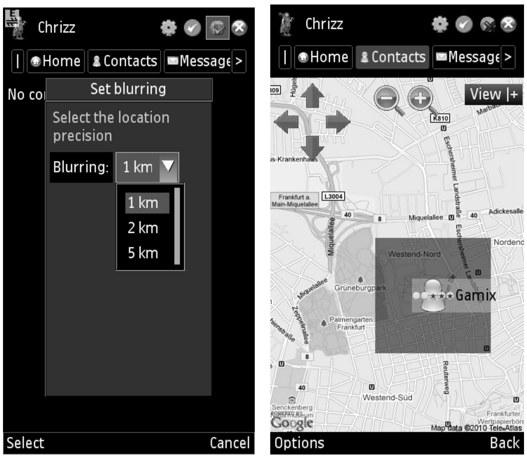
5.2.3. Location Blurring

The Location Blurring is handled via the location server in the platform and the Location Based Services in the client. In the status bar of the client, the user can turn on and off the GPS sensor or activate the blurring (by default GPS is deactivated). In the implemented application prototype a blurred position is displayed as a circle of a defined radius (e.g., representing 1, 2, or 5 km) randomly placed around the user's exact position, as shown in Figure 12.

The location sensor switch in the status bar is valid for all partial identities of the user (it is not possible to turn the location sensor off for a given single partial identity). If the switch is set to 'location blur', the partial identities are shown in the same blurring square but other users will not be able to determine, that they belong to the same root identity, because they could be at different places within the square.

5.2.4. Private Site

Private Sites are areas that have special meaning to their owner, e.g. home or work or in case of an angler a secret fishing spot. They consist of title, description, location and size and are only directly visible to their owner. The user defines his Private Sites via the client interface (Figure 13), which are stored as Site objects in



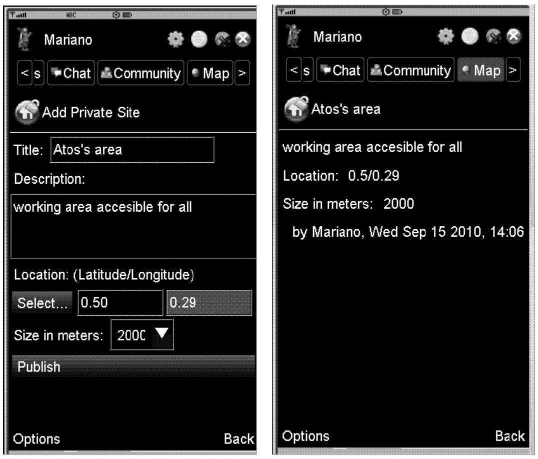
Select the location precision

Blurring: 1 km

1 km
2 km
5 km

Figure 12: The location-blurring feature.

the platform. A Private Site can be referenced in a policy, which means that the policy will be evaluated only if the owner's current location is inside the referenced Private Site.



Add Private Site

Title: Atos's area

Description:

working area accesible for all

Location: (Latitude/Longitude)

Select... 0.50 0.29

Size in meters: 2000

Atos's area

working area accesible for all

Location: 0.5/0.29

Size in meters: 2000

by Mariano, Wed Sep 15 2010, 14:06

Figure 13: Creation of a Private Site.

5.3. Testing

To validate the acceptability of the privacy enhanced technology concepts developed and implemented in PICOS, the community prototypes were intensively tested and trialled.

First, the angler prototype was tested in a lab and then in two field trials, in Vienna and Kiel respectively. The lab and field tests collected quantitative and qualitative data and evaluated the PICOS concepts realized in a mobile application regarding trust, privacy and identity management. Field tests have a similar procedure to lab tests, but they take place in the actual application context. To ensure active participation, several measures were taken by the PICOS team to encourage interaction and usage of the system. Since participants cannot be observed as in a lab test, they had to solve regular tasks, take notes, write diaries and fill in protocols. After the field tests, the participants were called back in the lab, where the experiences during the field test were discussed (Ganglbauer et al., 2010).The lessons learned from these first tests were used to improve the development of the prototype for the second trial cycle for another four week period at the same sites.

Lessons learned from the angling community were used to enhance the development of the Gamer prototype, which was trialled in Brno and Vienna, in a four week period. To achieve a realistic Gamer's scenario, all participants were active online gamers of Travian. Travian is a massively multiplayer online browser-based strategy game (Döbelt et al., 2010).

6. Findings

Presenting the results and findings, the conducted lab and field tests and the field trials showed that usability has to be considered as prerequisite of privacy-enhanced user interfaces and interactions. Therefore first the role of usability for implementing privacy trust and identity management features is viewed, followed by the appreciation of the features, and closing with general conclusions for privacy.

6.1. The role of Usability

Even though the focus of PICOS is not on usability, the results of the lab and field tests indicated that the privacy, trust and identity management functions cannot be comprehended without usable and logical interfaces and interactions.

For the lab and field tests, various instruments were used to collect data, observe, analyse and evaluate the usability. The "System Usability Scale" (SUS) (Tullis and Stetson, 2004) was used to measure the perceived usability of the system by the users. Furthermore, the feedback from the lab tests and the interviews that followed the tasks were considered. The SUS is a questionnaire which measures the subjective satisfaction of users who rate the usability of a technical system. Ten items are formulated as statements. The user can express his/her extent of agreement on a five point agreement scale (ranging from 1 = "I agree very much" to 5 = "I disagree").

The overall SUS rating for the clients running on mobile phones was between acceptable and good. In Kiel trial, the SUS questionnaire was repeated after the field tests, and for this the SUS rating dropped between "not acceptable" and "acceptable", compared to the rating collected in the lab tests. Naturally, more problems do occur during field tests than during lab tests, as real conditions always involve more potential problems than in controlled conditions. Long response times and reaction times were named as major problems during usage of the system.

To evaluate the user interfaces specifically for the PET technologies in PICOS, the PET-USES questionnaire (Wästlund et al., 2010) was applied. It enables users to evaluate user interfaces of privacy enhanced technologies with respect to their overall usability and measures six different PET-aspects in one usability scale. Users could rate according to their extent of agreement on a five-point agreement scale (1= I agree, 2 = I fairly agree, 3 = I'm not sure, 4 = I disagree, 5 = I strongly disagree). The following items were used to evaluate the PICOS application regarding the PET features of the application:

- *Data-management*. The extent to which the system makes it easier to store and organize personal information. This scale can be used to evaluate all types of identity management software and services.
- *Privacy Preferences*. The extent to which the system makes it easier to set general and excessive levels for data release policies and the extent the user is informed of unwanted data dissemination. Thus, an aspect of this scale is the decision support quality of the system.
- *Recipient Evaluation*. The extent to which the system helps users to evaluate credibility and trustworthiness of the data recipients. This scale can also be regarded in terms of decision support.
- *Data Release*. The extent to which the system clarifies what personal information is being released and who is the recipient of the data.
- *History*. The extent to which the system can show the user when, what, and to whom personal information has been released and thus provide an overview of what data any given service provider might have accumulated.

Results of the PET-USES questionnaire indicated that the participants in Brno and Vienna mostly "fairly agreed" on statements concerning the support of the application to learn and understand privacy related issues. Results of the mean values of the used PET-USES dimensions are shown for both trial groups in Table 3.

6.2. Appreciation of the features

The qualitative interviews showed that test participants appreciated the privacy-enhanced functions, especially the possibility to create private sub-communities. A private sub-community enables them to discuss certain topics only with a chosen set of friends, and only invited participants can join. Private sub-communities give the possibility to discuss certain topics and exchanging content within the community, without external users. The concept of retaining certain information or attributes from certain contacts on a very granular level was appreciated very much by the trial participants. Some of them argued that the list of privacy rules that a user is allowed to manage, could become confusing, if many rules were applied. The realization in the prototype, which demands horizontal scrolling through the overview of privacy rules, increased the confusion, as well.

Anglers		
	Feature	Frequency (%)
1	Location Based Services	83,3
2	Catch Reports	70,8
3	Water Course Advisor	45,8
Gamers		
	Feature	Frequency (%)
1	Location Based Services	76
2	Sub Communities	48
3	Partial Identities	44

Table 4: Most appreciated prototype features by community members.

The concept of Partial Identities was not appreciated by the users as much as the concepts of private sub-communities and privacy rules on a very granular level. Some participants did not appreciate this idea of Partial Identities, due to the fact that they were only participating in one community via the PICOS prototypes, and some participants of the angler trials were even strongly

Dimension	Mean Angler	SD Angler	Degree of agreement (A)	Mean Gamer	SD Gamer	Degree of agreement (G)
Data Management	2,46	0,30	fairly agree	1.87	0.57	fairly agree
Privacy Pref.	2,60	0,49	not sure	1.98	0.57	fairly agree
Recipient Eval.	3,00	0,33	not sure	2.62	0.55	not sure
Data Release	2,20	0,38	fairly agree	1.71	0.58	fairly agree
History	3,27	0,28	not sure	2.07	0.68	fairly agree

Table 3: Results of PET-USES questionnaire in Brno. The mean value and standard deviation (SD) are given for both Anglers and Gamers.

declining this function, as they do not feel comfortable to interact with anonymous users. In contrary most of the gamers appreciated the concept of Partial Identities and ranked it third regarding most appreciated prototype features, as shown in Table 4.

A prototype feature strongly related to this controversy on Partial Identities was the implemented reputation mechanism, where users could rate other users' contributions. For both trial groups, the concept of reputation was not clear to them and especially how the reputation was calculated. Participants did not transfer the reputation concepts of commercial websites to social networks. The users were unable to comprehend how a negative or positive reputation was calculated. Additionally it was unclear whether the root identity or the partial identity was rated.

In summary, the concept of the private sub-community and the Policy Manager were rated very useful in qualitative statements. The trial facilitators observed that the Privacy Advisor was not perceived as such, and it definitely needs a different presentation in the interface. The messages from the Privacy Advisor were perceived as confusing or interrupting for the flow of interactions. In the angling field trials the participants stated, that also the Privacy Manager was too complex. This feedback was picked up for the gamer prototype and the process was simplified by offering a wizard to create privacy rules, which was well accepted in the gamer's trial. Additionally the Privacy Manager received some positive feedback, for giving a good overview on the already applied rules.

Furthermore the field trials indicated that users appreciated a lot the Location Based Services as well as the Catch Report functionality including the possibility to blur a location, as shown in Table 4. The exchange of Catch Reports and posts in the public forum were mentioned as most central and appealing during the trials. The trial users appreciated the possibility to restrict unwanted access to their location and fishing spots or to apply a blurring to their location and the location of a fishing spot respectively. Especially the anglers could imagine using those features for angling specific activities. In comparison, the gamers rated the Locate Buddies service most appealing during the trials and proposed the improvement of blurring by adding a broader range to blur their position or set a range by their own.

Table 5 shows how much the features were actually used by the users during the trials. Interestingly enough, this does not match with the way users has expressed their interest and appreciation of the features during the interviews. For example, although being the most appreciated feature, the Location Based Services were not the most used feature in both communities. Instead, asynchronous messaging in form of public communities for the anglers and sending messages for the gamers, was the most used functionality. What is also interesting to note is that for the anglers, the Sub Communities were used in practice more than Location Based Services, even though this feature is not even present in the three most desirable features of Table 4, showing the need of the users to preserve their privacy. This is explained by the fact that in reality, anglers preferred to share information about their catches with their biddies within the Sub Communities and not just with everyone.

Anglers		
	Feature	Frequency (%)
1	Public Communities	75
2	Sub Communities	50
3	Location Based Services	29
Gamers		
	Feature	Frequency (%)
1	Send Messages	73,33
2	Location Based Services	60
3	Sub Communities	53,33

Table 5: Most used prototype features by community members.

Concluding, the participants generally evaluated the privacy enhancing features (e.g. the option to switch between Partial Identities or the blurring function) as positive and regarded them as a special advantage of the application. In general, the users appreciated the implementation of privacy concepts, but saw their application in a much broader context than in one single community. However the trials also showed that the Angling and the Gaming Community have different requirements in relation to technical needs and features. In contrast to the anglers, the gamers mentioned, that they would appreciate different ids in different online environments. This makes sense, if one considers the fact that gamers are involved in more online communities compared to the anglers, who tend to register in one angler online community and stick to this for a longer period.

In both communities, one thing emerges as the strength of the PICOS mobile application: many of the features which were mentioned as a highlight from the angler trial participants, were also mentioned from the gamer trial users (e.g. private sub-communities, Location Based Services such as blurring, show contacts on map, the dedicated visibility to other community members etc.).

The major differences between the angler and gamer community were how the users perceived the PICOS concepts regarding their usefulness for other web resources and mobile applications. Members of the gaming community perceived the PICOS concepts as an add-on for all kind of social communities and suggested their extension to other application fields, so that people can benefit most by Partial IDs. On the contrary, the angler community appreciated the improvement of privacy and data management provided by the PICOS features for their own online angling community and the corresponding mobile applications.

6.3. General Conclusions for Privacy

The research on privacy in mobile communities and the results of the PICOS community prototypes trials show that new privacy enhancing concepts in the mobile environment are needed besides already established concepts. Combinations of those new and established concepts lead to innovative features that enable the user to manage his privacy in a convenient way. For instance a combination of the concept of Partial Identities with Access Control allows a secure and private communication in sub-communities. In sub-communities, users can communicate asynchronously with their Partial Identities without the need to check continuously who is allowed to read. The Access Control manages that the access rights for content in the sub-community only need to be set once.

Automation for privacy settings is important for mobile communities. Especially on mobile clients with their limited interfaces, automation can support the reduction of complexity of privacy settings by reducing the need for manual configurations. Especially, in a mobile environment the context changes very often due to the movement of the users. Thus, in a mobile environment users need to adapt their privacy settings more often compared to a fixed-line environment. A combination of Blurring and Privacy Manager helps the users to further reduce the complexity. With the help of the Privacy Manager users can configure in detail when, towards whom, to which degree and in which context his location will be obfuscated. All rules can be previously defined as well as adapted on the go, if needed.

Another example for the reduction of complexity is the previously described concept is the Private Site. In this case users just need to mark a point on a map. With this simple interaction the user's position is always hidden when he is at this location. The PICOS user trials have shown that users like to have such kind of automation for privacy settings to reduce the complexity of managing their privacy. Besides the mentioned examples, further features to support users have to be investigated.

For further reduction of complexity and in order to improve the comprehensibility, privacy concepts need to be oriented to the "language" of the different kinds of communities. For instance the use of metric values in the blurring feature was no problem for anglers. In their daily life they are using metric values and can easily work with them. For other communities, like the online gamers, this is not necessarily the case. For our trial group of online gamers it was hard to assess the dimensions of metric values. Therefore, less abstract values were needed, as for example street, district, city, etc. To let the user choose out of non-abstract values can support him in understanding privacy concepts. Therefore, consideration of the vocabulary of the communities when building appropriate privacy concepts will lead to better understanding of the concepts.

The assessment of privacy was also a problem for PICOS test participants until the end. Many of them were not concerned about privacy, as long as they were not directly confronted with it. As a result from the user trials it was found out that users' awareness regarding privacy needs to be raised further. Users need to be supported in controlling the disclosure of personal information, while being able to use services. Even though PICOS was not able to address all of the relevant aspects in this context, we made an important step with the concept of the Privacy Advisor, which demonstrates how to address the need of such support.

7. Summary and further work

In this paper we outlined why there is an increasing need for privacy and identity management related enhancements in mobile communities and motivated why research is necessary in this application area. Based on the process of gathering user requirements, we described how to achieve such enhancements with advanced concepts of privacy and identity management, and their integration in a community platform architecture. We explained some exemplary privacy enhancing concepts and described how such concepts were prototypically implemented, trialled with end users and evaluated. Besides the actual privacy enhancing concepts we also showed the technical feasibility for the delivery of targeted advertising and its integration with the privacy enhancing concepts. The trial and evaluation results helped us derive some general findings with regard to the researched aspects. This will provide a basis for applying PICOS concepts to various existing mobile community services. Furthermore, the prototype development process in PICOS affirmed that the Privacy by Design principle is an indispensable strategy for embedding privacy features into a system.

However, further research is needed with regard to particular aspects. In our research we focused on the relationships and interactions between users in mobile communities, and associated privacy and trust issues. Further research is needed regarding the relationship between users and the community operator, respectively the community service providers and associated privacy and trust issues (e.g. use of user data by the community operator). Further research on the usage and benefits of the privacy enhancing concepts needs to be conducted. Especially how these concepts can be applied in a user friendly and comprehensible way to existing social networks and which further involvements might be needed to address emerging privacy challenges (e.g. due to new context-based services). Risk and financial assessments of integrating PETs in community platforms for a community provider would also provide further transparency.

Also in the field of advanced marketing and advertising mechanisms for communities, additional research activities are needed. Research in this area so far mainly considers specific aspects of marketing or advertising (e.g. viral marketing). Holistic approaches are needed, in order to cope with the complexity of community structures and to consider the different stakeholders and their possibly diverging interests in social networks as well as the factors which influence the success of marketing activities. Such approaches might need to be adaptable to specific products or services, which are subject to marketing activities. Also the optimization of business models for the delivery of targeted advertising can be subject to further research.

Additionally, mobile devices are more and more used to manage the data-overflow of user related information. Especially, recommender systems that are selecting special places (like restaurants, bars, etc.) fitting to users' preferences can help to manage this data-overflow. Beside the fact that users are interested to get support by using those services, it is not always transparent which personal information recommender systems need and use to find out preferences of each user. How to manage the privacy of users' community profile in the case of such recommender systems is also question to be answered.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2011) under Grant Agreement n.215056.

References

Adu-Oppong, F., Gardiner, K., Kapadia, A., Tsang, P., 2008. Social circles: Tackling privacy in social networks, in: Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08), Pittsburgh, Pennsylvania.

Arlinghaus, R., Mehner, T., Cowx, I., 2002. Reconciling traditional inland fisheries management and sustainability in industrialized countries, with emphasis on europe. Fish and Fisheries 3(4), 261 – 316.

Barkhuus, L., Dey, A., 2003. Location-based services for mobile telephony: a study o users privacy concerns, in: Interact, Zrich. pp. 497–506.

Beales, H., 2010. The value of behavioral targeting (study).

Caradec, J., 2010. D5.2b Platform Protoype 2. Public Deliverable of EU Project PICOS.. Available at www.picos-project.eu/Public-Deliverables.29.0.html (2010).

Chew, M., Balfanz, D., Laurie, B., 2008. Undermining privacy in social networks. Web 2.0 Security and Privacy (in conj. with IEEE Symposium on Security and Privacy) .

Clavedetscher, C., 1998. Point: User involvement key to success. IEEE Software, 15(2),, pp. 30, 32.

Dobele, A., Toleman, D., Beverland, M., 2005. Controlled infection! spreading the brand message through viral marketing. Business Horizons 48(2), 143–149.

Döbelt, S., Überschär, B., Alvarez, M., Heim, S., 2010. D7.3 Second Community Prototype: Trial Report. Public Deliverable of EU Project PICOS. Available at www.picos-project.eu/Public-Deliverables.29.0.html (2010).

Ganglbauer, E., S., D., Überschär, B., 2010. D7.2a First Community Prototype Lab and Field Test Report. Public Deliverable of EU Project PICOS. Available at www.picos-project.eu/Public-Deliverables.29.0.html (2010).

Görlach, A.; Heinemann, A.T.W., 2004. Survey on location privacy in pervasive computing. Privacy, Security and Trust within the Context of Pervasive Computing, The Kluwer International Series in Engineering and Computer Science , 23–34.

Hansen, M., Berlich, P., J., C., Clau, S., Pfitzmann, A., Waidner, M., 2004. Privacy-enhancing identity management. information security technical report 9(1), 35 – 44.

Hartline, J., Mirrokni, S., Sundararajan, M., . Optimal marketing strategies over social networks, in: Proceedings of the International World Wide Web Conference Committee 2008 (WWW 2008).

Hiltz, R., Passerini, K., 2007. Trust and privacy concern within social networking sites: A comparison of facebook and myspace, in: Proceedings of AMCIS 2007.

Ho, S., Kwok, S., 2002. The attraction of personalized service for users in mobile commerce: An empirical study. ACM SIGecom Exchanges Vol.3 No.4,, 10–18.

Hoegg, R., Martignoni, R., Meckel, M., Stanoevska-Slabeva, K., 2006. Overview of business models for web 2.0 communities, in: Proceeding of Workshop Gemeinschaften in Neuen Medien (GeNeMe), Dresden. pp. 33–49.

Holzblatt, K., Beyer, K., 1995. Requirements gathering: the human factor. Communications of the ACM 38(5), 31–32.

Kahl, C., Albers, A., 2010. Towards reasonable revenue streams through marketing in mobile social networks, in: Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI), Gttingen, Germany.

Kempe, D., Kleinberg, J., Tardos, E., 2003. Maximizing the spread of influence through a social network, in: Proceedings of Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD '03), Washington, DC, USA.

Kotler, P., Armstrong, G., 2006. Principles of Marketing. Prentice Hall, New Jersey, Upper Saddle River, USA.. 11th edition.

Leskovec, J., Adamic, A., Huberman, A., May 2007. The dynamics of viral marketing. ACM Trans. Web 1,1, Article 5.

Liesebach, K., Scherner, T., 2008. D2.4 Requirements. Public Deliverable of EU Project PICOS. Available at http://www.picos-project.eu/Public-Deliverables.29.0.html (2008).

Müller, G., Wohlgemuth, S., 2005. Study on mobile identity management.

Nielsen, 2009. Global faces and networked places - a nielsen report on social networking's new global footprint.

Palmer, A.; Koenig-Lewis, N., 2009. An experiential, social network-based approach to direct marketing. Direct Marketing: An International Journal Vol. 3 No. 3, 162 176.

Phelps, E., Lewis, R., Mobilio, L., Perry, D., Raman, N., 2004. Viral marketing or electronic word-of-mouth advertising: Examining consumer responses and motivations to pass along email. Journal of Advertising Research vol.44 no.4, 333–348.

Pousttchi, K., Turowski, K., Wiedemann, D., 2008. Mobile viral marketing - ein state of the art, in: Bauer, H.H.; Dirks, T.B.M. (Ed.), Erfolgsfaktoren des Mobile Marketing. Strategien, Konzepte und Instrumente, Springer, Berlin. p. 289304.

Preibusch, S., Hoser, B., Gürses, S., Berendt, B., 2007. Ubiquitous social networks - opportunities and challenges for privacy-aware user modelling, in: Proceedings of the Data Mining for User Modelling Workshop, Corfu.

Rumbaugh, J., 1994. Getting started: Using use cases to capture requirements. Object-Oriented Programming Journal 7(5), 8–12.

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J., 2009. Understanding and capturing people's privacy policies in a mobile social networking application. Personal Ubiquitous Comput. 13, 401–412.

Schulz, S., Mau, G., Löffler, S., 2007. Virales marketing im web 2.0, in: Springer (Ed.), T. Kilian, B. Hass & G. Walsh (Hg.). Web 2.0 Neue Perspektiven im E-Business, Heidelberg. pp. 249–268.

Subramani, M., Rajagopalan, B., 2003. Knowledge sharing and influence in online social networks via viral marketing. Communications of the ACM 46:12, 300–307.

Tullis, T., Stetson, J., 2004. A comparison of questionnaires for assessing website usability, in: Usability Professional Association Conference.

Wästlund, E., Wolkerstorfer, P., Köffel, C., 2010. Pet-uses: Privacy-enhancing technology users self-estimation scale, in: Bezzi, M., Duquenoy, P., Fischer-Hbner, S., Hansen, M., Zhang, G. (Eds.), Privacy and Identity Management for Life. Springer Boston. volume 320 of *IFIP Advances in Information and Communication Technology*, pp. 266–274.