Privacy and Community Connectedness: Designing Intelligent Environments for our Cities

Author

Chatfield, C, Hexel, R

Published

2007

Conference Title

Australasian Computer-Human Interaction Conference, OZCHI'07

Privacy and Community Connectedness: Designing Intelligent Environments for our Cities

Craig Chatfield
Griffith University, School of ICT
Smart Internet Technology CRC
Brisbane, Australia
+61 7 3875 7990
c.chatfield@griffith.edu.au

René Hexel
Griffith University, School of ICT
Smart Internet Technology CRC
Brisbane, Australia
+61 7 3875 5041
r.hexel@griffith.edu.au

ABSTRACT

This paper investigates the casual interactions that support and nourish a community and seeks to provide a solution to the increasing detachment of modern society as community spaces become less and less engaging. We suggest the use of a ubiquitous computing (ubicomp) infrastructure to promote and support community connectedness via the hosting of virtual community environments and by providing local information and interaction possibilities. This infrastructure addresses our need as society to communicate more effectively and create loose bonds with familiar strangers within our community. We explore this idea with a use scenario and user study of users interacting with the services in a developed intelligent environment.

Categories and Subject Descriptors

H.5.3 [**Information Systems**] Group and Organisation Interfaces.

General Terms

Design, Human Factors, Theory

Keywords

Privacy, Ubiquitous Computing, Community, Third Places

1. INTRODUCTION

In his book 'The Great Good Place' Ray Oldenburg describes the impact of 'third places', e.g. coffee shops, libraries, clubs etc., where community members meet and interact. Third places promote casual social interactions between community members and are 'at the heart of a community's social vitality and the grassroots of democracy' [1]. But today's communities are losing their third places to the suburbanisation of our cities, which limits access to third places, and to the increasing cost of entertainment or 'going out', which alters a third place's nature, accessibility and social value. This loss has eroded the social, economic and personal benefits people derive from casual interactions with their community.

OzCHI 2007 Proceedings, ISBN 978-1-59593-872-5

As our societies lose places for casual interaction amongst people, there is a trend towards individualism and disengagement from the greater community. The traditional sense of 'community' is being replaced by personally centralised groups of friends and family that maintain their own sense of community. These collectives, variously described as social networks or urban tribes [2], provide the support and casual interactions 'missing' from modern urban environments. Wellman describes this change from place-to-place to person-to-person communication as Networked Individualism [3], in which micro-communication with our 'tribe' replaces casual social interaction with our community.

These urban tribes, via new communication methods and evolving social practices, are supplementing or replacing the socialisation that once took place in 'third places'. Through friend-of-friend associations and the overlapping of different social groups, people are exposed to wide range of people similar to community gatherings in public space. This new phenomena could be called a symptom of the modern community, or of modern communication tools (i.e. it is now possible to maintain contact with a select group of friend and to spurn all contact with the community). Any solution to improve community interaction should address not only the lack of third places in our communities, but should also leverage the interactions and relationships within our urban tribes.

Intelligent environments are highly embedded, interactive spaces that seek to bring computation into real world physical spaces [4]. Existing intelligent environments provide users with personalised environmental information [5], m-commerce service delivery [6], and information sharing with our friends and colleges [7, 8, 9]. Intelligent environments could and should do more to support community connectedness in our everyday environments, but any solution must acknowledge the number of privacy issues with the capture, storage and use of personal information within ubicomp environments.

This paper examines how the community integration and social connectedness supported by third places can be improved using intelligent environments. We begin by examining the specific characteristics of third places that promote social interaction and investigate what difficulties typically occur in the development and support of successful 'virtual' third places. Section three examines the development of an infrastructure of overlapping intelligent environments, including the privacy and community interaction concerns. It then highlights the community interaction requirements for this infrastructure describing a use scenario, and suggesting a potential interface to encourage community engagement. The paper concludes with a user study investigating users' perceptions of the services and the ubicomp infrastructure.

2. COMMUNITY CONNECTIONS

Oldenburg believes that America has a ‘problem of place’ because ‘the automobile suburb has the effect of fragmenting the individual’s world’ [1, p. 4]. The benefits third places have upon a community are slowly being eroded by compartmentalised town planning and changes in consumer’s lifestyles and community interaction. But the nature of third places makes them difficult to replicate or support using technological means. To consider how we might provide this support, it is useful to consider the specific characteristics of Oldenburg’s third places:

- They are on neutral ground
- They are a social leveller
- Conversation is the main activity
- They are accessible
- They act as a home away from home and have ‘regulars’
- The mood is playful

Attempts have been made to recreate third places using computer-mediated communication (CMC) environments like chat rooms, multi-user environments or bulletin board systems (e.g. [10, 11]). Soukup [12] provides us with a systematic evaluation of the extent to which CMC systems’ (or ‘virtual communities’) fulfil the roles of the third place. Virtual communities do provide a neutral third place away from the demands of work and home life [11] where regulars can meet for ‘playful and fun’ conversations or interactions [10]. This playfulness is often promoted by the types of interactivity and identity concealment (or use of a persona) common in virtual communities [13]. But Soukop [12] identifies three problems with these computer-mediated environments: they don’t emphasise a localised community, they don’t provide a social levelling place of interaction, and they are not accessible.

Oldenburg asserts the importance of geographically situated community interaction in his second edition preface: ‘The first and most important function of third places is that of uniting a neighbourhood’ [1, p. xvii]. But computer-mediated environments are rarely used by member of the same physical community, indeed they ‘are unique because they *transcend* physical space, offering communication opportunities outside their community’ [10]. Any ‘virtual third place’ must therefore be either physically collocated in the local community, or should be primarily used by members of the community while discussing issues relevant to that community. Virtual communities tend to have specific target audiences based upon a common set of interests or beliefs (e.g. Entertainment, Sporting, Religious or Political topics) while third places suggest a commonality based upon where people live. The latter leads to an informal meeting place where social positions tends to be less important, while the former leads to knowledge-based social hierarchy counter productive to relaxed social engagement and community integration [10].

Accessibility of the third place by all is also essential for greater community involvement and integration. Access to ‘virtual communities’ are, by definition, limited to those with access to the internet. This creates barriers of access, and prevents the engagement of the entire community. But technological access alone is insufficient to solve accessibility problems. Virtual communities are much more effective when coupled with well designed (and culturally aware) training [14], and social connection and informal interaction are essential to promoting community interaction and participation [15]. Third places should also be constructed by (or in consultation with) participating members of the community.

Soukup identifies ‘presence’ as a final requirement of ‘virtual third places’ in constructing a welcoming home away from home. Presence describes the ‘sense of being in an environment’ [16] or the degree to the virtual third place promotes users’ to feel immersed in the environment [12]. This sense of immersion is integral to users acceptance and ownership of the space, and will determine the extent to which the community becomes engaged in the environment. Environments should look and feel (as much as possible) like the communities they represent, and creative use of animation, three-dimensionality and characterisation of identity (e.g. Avatars or personas) should be used to enhance the process of localisation and presence [12]. These guidelines highlight the importance of connecting the user to the community, and not of the delivery of a complete multimedia experience.

3. UBICOMP INFRASTRUCTURE

3.1 Intelligent Environments

Marc Weiser described the trend of embedding miniaturised computing devices within everyday objects and environments as ubiquitous computing [17]. Intelligent environments describe any physical spaces that provide contextually aware ubicomp services. The P3 Framework [18] examines context-aware community and user-based interaction systems that are either people or location centric. These systems support personal interaction such as opportunistic communication with colleges and friends, social matching and the maintenance of social networks. Place-centred services include social navigation, task coordination and communication about places and activities. This research seeks to develop a ubicomp infrastructure that supports users with context-aware services across multiple areas of their lives (e.g. transport networks, home, office, shopping centres, etc.).

Many intelligent environment architectures have been developed [e.g. 5, 19, 20], but they primarily focus on the technical requirements for correlating user information and managing interactions within their environments. The Confab toolkit [9] expands on previous privacy work and facilitates the development of privacy-aware applications to end-user and application developer’s requirements. This work provides guidance on the development of ubicomp applications but fails to consider how the environments might form a complete ubicomp infrastructure.

Ubicomp has the effect of spreading computers throughout the environment while effectively making them invisible to users [17]. The invisibility problem describes the conflicting goals of ensuring ubicomp blends naturally into the background [21] with the need to draw the attention of users to its services. This can be solved through the personalisation of the service interface [5], allowing the system to recommend services based upon stated or observed user preferences, but this raises privacy concerns relating to the collection, storage and reuse of this information.

Intelligent environments tend to use handheld computers (e.g. PDA or mobile phone) to communicate wirelessly with the environment. The ActiveCampus project [22] is a ubicomp environment with community interaction, directions and local information services. The ActiveCampus project demonstrated the benefits of improving community interaction inside classrooms, but privacy issues remained with users’ overwhelmingly (91.5%)

rejecting exchanging location and presence information with other (non-buddy) users.

3.2 Privacy within Ubicomp

Privacy is an important concern when designing intelligent environments. Due to their pervasive nature these environments have an unprecedented ability to gather information about all aspects of a users life [23]. Subsequently users' unwillingness to trust ubicomp systems is seen as the major impediment to acceptance of these systems [24]. This comes at a time of increasing identity theft and digital fraud, and during changing social attitudes that have lead us to more isolationistic behaviour. Oldenburg identifies the replacement of the 'facilitating public etiquette consisting of rituals necessary to the meeting, greeting, and enjoyment of strangers' with a 'set of strategies designed to avoid contact with people in public [utilising] devices intended to preserve the individual's circle of privacy against any stranger that might violate it' [1, p. 13]. Our intelligent environment architecture must balance this desire for privacy with our goal of supporting greater social inclusion and community connectedness.

User privacy is not, however, the exclusion of information sharing with others, it is, in fact, the ability of an individual or group to determine themselves when, how and to what extent information about them is communicated to others [25]. Studies of user privacy within intelligent environments have found users want control over any information sharing [8, 26, 27], require a greater awareness of an environment's owners [28] and the privacy policies applied to any collected information [26, 27, 28] and want collected information's use to be limited to the current environment [28, 29]. More generic privacy investigations have described these goals as improving the flow of information to the user, whilst limiting the flow of information about the users into the environment [30].

An 'Identity Manager' is an application that enables each user to express and to enforce his or her privacy and security needs in IT-systems depending on the situation the user is in [31]. User should be able to manage the exposure any entity has with a portion of their identity, whilst allowing repeatable interactions for service personalisation. Confirmation of identity is often required by ubicomp services, and should be provided using third-party identity brokers (e.g. a bank or government department). Methods of supporting partial identity recognition, like the confirmation of the user's birthday without releasing their name, should also be available, and users should be able to reproduce real-world interaction possibilities, like making an anonymous purchase, without requiring extra information that could be captured for future use.

Privacy within intelligent environments involves the delivery of information to users to allow them to make their own privacy determinations. Users' preferences for what information is valuable will provide some variation on what is considered an acceptable information exchange. Users should not maintain the sole responsibility for their privacy, however, as they consistently act against stated privacy preferences when offered something of (perceived) value [32]. This has caused the call for 'privacy minimums' [33] to be implemented into ubicomp environments to protect users where possible from unintended privacy breaches. An intelligent environment architecture must dually provide users with an anonymous interaction infrastructure, and providing users with enough information to determine any unacceptable risks to their privacy whilst utilising an environment's services.

3.3 Interaction Design Requirements

This section considers the interaction requirements for our intelligent environments and the greater ubicomp infrastructure. Users' privacy concerns suggest that our infrastructure must allow anonymous interactions and provide technical security to the prevent tracking of users or the exposure of their personal information. The types of services that will be supported will also dictate the interaction possibilities required by users, and the necessary identity management structures. In particular we will consider the impact of using ubicomp environments on the localisation, accessibility and presence of virtual third places.

The use of ubicomp environments to provide user interaction spaces addresses some of the primary concerns of creating virtual third places simply due to their contextualisation in a physical space. Intelligent environments cover a particular physical location, so users accessing the virtual third place are actually present in the community. This localisation of the virtual community provides the users with an actual sense of 'presence' which allows them to relate more effectively to the virtual community, improving its potential effectiveness as a virtual third place. This sense of 'presence' may be reduced if access to the community environment is made available to users outside the physical environment.

Intelligent environments are accessed using mobile phones or other handheld computing devices (e.g. PDAs, smart phones) from within the physical environment. External access to these environments is often restricted (depending on their purpose), which means most users would be physically situated within the environment, heightening its relevance to the local community. This ease of access, and openness to all users should promote the 'social levelling' experienced in physical 'third places'. Additional access could be provided via the internet, but while this would improve the community's access to the interaction environment, it would reduce the sense of presence users feel when interacting from within the physical community. Users should have complete control of their identity for this interaction, and should be allowed anonymous or avatar-based interaction to promote the sense of playfulness and accessibility.

A ubicomp infrastructure could support community interaction by hosting existing virtual community forums. Discussion boards, chat rooms and multi-user domains could all be used for (localised) virtual community interaction. Second Life (www.secondlife.com) is a virtual world that allows users to create their own landscapes, interact with other users and recreate most real world activities. MySpace (www.myspace.com) and YouTube (www.youtube.com) provide interaction forums nominally based around interaction and the sharing of multimedia content. Each of these could be adapted to an ubicomp infrastructure to promote interaction in real third places. Experience with mixed-reality games further demonstrates the benefits of providing a communication channel for users within an ubiquitous computing supported environment [34]. In these environments this channel was used to allow users to share local information, provide technical support to other users, and to coordinate strategies for achieving a common goal.

Additional environmental services could provide local directions, background information and notices of community group meetings. For example environmental services could identify local meeting places, provide local background information to foster a better sense of community and identify regular (formal and informal) meetings of groups and associations. A further (optional) service might provide public information on the environments occupants, which could promote better community interaction by reducing barriers of interaction with strangers. Again we suggest this will only be successful if users have complete control of their public identity personas or the 'face' [35] that they present to the environment. Confirmation of users identity will be required for some services, e.g. to purchase goods or confirm the users identity, which requires a centralised method of confirming partial identities across the entire infrastructure.

Supporting user interaction amongst their urban tribe requires us to look past existing communication and awareness tools like Instant Messenger (IM), Voice over IP (VoIP) telephony software and email. Whilst these tools will be useful, and ideally accessible via the ubicomp infrastructure's internet access, ubicomp services will allow more effective communication with the user's group of friends (or urban tribe). Ubicomp services can locate nearby friends, coordinate calendars or schedules and provide awareness of the group's activities. These tools require access to a central server, most likely via the internet. Providing internet access through the environment would add further value to any such environment and assist in building user acceptance of the infrastructure.

3.4 SPACE Architecture

The Scalable Privacy Aware Communication Environment (SPACE) architecture is a scalable intelligent environment architecture that was developed from previous work described in [35]. The SPACE architecture provides a secure, anonymous interaction framework in which services can be delivered to users' handheld computers (e.g. PDAs, smart phones, etc.). The architecture provides users with secure methods of selectively exchanging their personal information, allows users anonymous interaction with the environment and uses third party identity management to validate service access. A proof-of-concept implementation was developed in Python to test the architecture and to ensure privacy and security goals were met.

The SPACE architecture provides a scalable infrastructure that can seamlessly integrate ubicomp services into our everyday environments. To avoid the excessive collection of user information, the intelligent environment's user management and service delivery components have been separated, and all information requests made of the user are routed to an online user controlled proxy (an online server controlled by user set preferences) via an anonymising third party. This prevents the identification of the user via traffic analysis, and provides a permanent access point for managing interaction with the greater ubicomp infrastructure. This is useful for managing interactions with the user's urban tribe via IM, VoIP or other group awareness services.

Methods of proving and sharing identity are especially important in intelligent environments. To allow users to confirmation their identity with a service, irrespective of the environment, global identity structures must be utilised. Identity Brokers provide global confirmation of user identity similar to real world government agencies or a digital certification company (e.g. Verisign). User's can also exchange verifiable personal information by using digitally signed user profiles [36] (or personas) for personalised pseudo-anonymous service access. The templates are digitally signed by the issuing company, and the the intelligent environment makes a trust evaluation of the issuer when determining whether or not to accept the digital template. Users use these to interact with a service (or group of services) with only a specified subset of their user information, further reducing potential risks to their privacy.

The SPACE architecture uses multicast DNS (mDNS) beacons to broadcast the existence of intelligent environments and their services to users. Users' handheld computers then personalise the interface based upon the user's environmental and service preferences. Users can interact with these environments anonymously, until there is a reason for exchanging personal information. The SPACE architecture uses Kerberos to manage the communication between users and the environment. The Identity Broker acts as a key distribution centre for exchanging encryption keys and managing access to restricted services and interaction between users. The intelligent environment's public key is also provided (using the mDNS beacons to publish its location) to allow users to begin conversation with an environment prior to the key distribution or in the event of loss of internet access.

This method of interaction allows users to remain in control of their personal information at all times. It allows users to selectively share information and services with other users, via their personal domains, even where internet access with their handheld may be inadequate or patchy. Users maintain control of their identity, and can selectively share any portions required for service access (e.g. over 18) without providing all their personal information. These structures allow users complete control over their interaction with an environment, and this allows users to integrate the use of available ubicomp services into their everyday lives without exposing them to risks to their personal privacy.

4. COMMUNITY INTERACTION

As wireless networks are increasingly implemented on city-wide [38] and country-wide scales [39], a ubicomp infrastructure that covers our everyday lives becomes possible. This infrastructure could be utilised to promote a greater integration of the community and more effective use of virtual and real third places. Ubicomp services could provide local information, enhance community coordination and provide virtual third places for interactions by community members. By using ubicomp environments to host and access these virtual communities we overcome some of the short comings of accessing virtual communities using more traditional computing devices.

Central to the privacy requirements of using ubicomp environments is users' explicit control over their information's use and distribution. The standard information (or public profile) provided to the intelligent environment should be descriptive, non-unique and designed to engage with other members of the community. Contact information could easily be integrated into this system, but should be sharable only with the explicit consent of the user. For greater security, this exchange could occur locally without involving the network (via Bluetooth, IR or other wireless protocols). It is hoped that the user interface will take some steps to address the anonymous nature of crowds in our larger cities and reduce the barriers to interacting with strangers observed by Oldenburg. We do not believe this interface will double as a dating service, but we look forward to the natural evolution of use that inevitably occurs with any new communication tool.

If this community interaction interface is to be successful it must be widely available, and must be easy to use and valuable for its users. The increasing costs and ultimately exclusive nature of commercial systems suggests a publicly funded or not-for profit model would be more effective at supporting and creating the essential elements of successful third places. Ubicomp services that add value to the infrastructure (e.g. local information access, internet access etc.) will further increase the community interest and engagement in the infrastructure and promote its success. Conversely fee-based or service poor systems would discourage participation and make the infrastructure less effective.

4.1 Use Scenario

To provide a more grounded discussion on this infrastructure, let us consider an intelligent environment proposed for the Kangaroo Point cliffs area of Brisbane, Australia. The site of an old quarry along the Brisbane River, this area provides recreational rock climbing, boating and sporting facilities to the general public. A social area used by many as a third place, this environment could benefit from a ubicomp infrastructure to provide local area information, highlight local activities and climbing group meetings and provide other communication and location-centric ubicomp services. An interface to access the environment's services would allow users to access their personal network (or urban tribe) via group communication and awareness tools, see and manage their shared identity, utilise the environments' services (e.g. accessing a community discussion board or commercial service) or receive information on the local area.

Consider the following scenario of using the suggested user interface (refer to Figure 1) to explore the area and interact with the local community. Belinda has recently moved to Brisbane to start university and is exploring the city. Upon entering the environment the 'Local Area' screen shows Belinda all users logged into the environment with a 'public face' selected. If Belinda chooses, she could also select to remain anonymous, but hoping to meet new people she selects her usual profile describing her and providing a picture. If there were lots of users in the area,

Figure 1. 'Local Area' User Interface Screen

she could filter the users to only show people that met some specified criteria (e.g. users over 20). Walking along the base of the cliffs, Belinda notices a climber that matches a user profile's picture, and she approaches him and strikes up a conversation.

Belinda could use the 'Services' tab to access the services provided in this intelligent environment (refer to Figure 2). Each service is displayed with links to relevant information and any available interaction and personalisation histories. Selecting a service loads the interface maintained by the service provider, using the identity set using the 'ID Manager' interface. Services could be colour-coded in this interface so users can identify different service types at a glance.

Figure 2. 'Services' User Interface Screen

When connecting to the environment, Belinda's PDA connects her to her social network which updates her location on its server and returns a list of all her friends currently connected to the service (i.e. displayed in the 'Contacts' tab). A few minutes later a warning beep informs her that a friend has just entered the nearby area, and she sends them an instant message to see if they want to meet up. Belinda's friend suggest they meet at the boat house, and not knowing where this is she selects 'More Details' on the 'Local Area' screen. This prompts the systems to display a map, some local information and a short history of the area. As she finds the boat house Belinda notices in the local information that a climbing group meet regularly at the cliffs and she makes a note to join them next time she's available.

5. USER STUDY

A user study was developed to investigate users' use of ubicomp services within a familiar everyday environment. Users were invited to interact with two intelligent environments providing users with environment-specific services and access to local information. The study was unable to examine community interaction with virtual third places due to the necessarily longitudinal nature of the study, and due to the unavailability of this feature in our implementation. A user interface was developed in mod_python and was accessible via a web browser on handheld or traditional computing devices.

The user study (N=18) consisted of exploring the two intelligent environment's services, covering a common use computing facility and the greater university campus area, and answering questions on the experience. Volunteers for this study were recruited on the basis that they would likely be early adopters of technology, so we sought out accessible, young people familiar with information technology. This was reflected in our survey population which were mostly students under the age of 30 (72%), identified themselves as in the IT field (83%) and owning a mobile phone or PDA (89%). No financial compensation was provided to the eleven men and seven women participants.

After a briefing on the nature of the intelligent environments, user pseudonyms, and the Service Interface (see Figure 3), users logged into each environment and investigated the available services. Users were able to select three different levels of anonymity (e.g. the Anonymous, University Certified and Identifiable pseudonyms), which demonstrated the escalating levels of service access. (The University Certified pseudonym allowed the environment to identify the user was enrolled, and therefore entitled to access university services, but did not provide any personal information). After becoming familiar with the environment's services users were asked to answer questions on their interaction. (A list of questions asked can be found at http://www.cit.gu.edu.au/~craig/questionnarie.html).

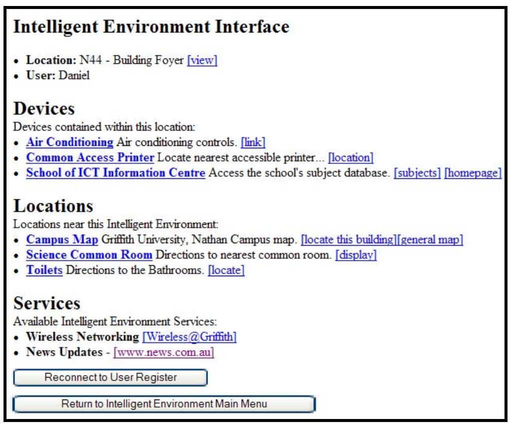

Figure 3. User Study Intelligent Environment Interface

All users indicated that the intelligent environments provided valuable services. Primarily users liked the direct and easy access to local information (e.g. Maps, directions etc.) and the ability to control what information the environment knew about the user. Users also enjoyed the collection of links to useful, external services (e.g. News, Weather, Internet Search Engines etc). User feedback highlighted the need for a more graphical interface and for better feedback on the use and maintenance of user pseudonyms. Users were also keen to see the interface ported to mobile phones to allow for better integration into their lives.

To further illustrate the use of pseudonyms in this environment, a more advanced interface was shown, containing more information on each pseudonym (Figure 4), particularly the information associated with each pseudonym, and the type of interaction and feedback possible. Upon reflection, all users agreed that this use of user pseudonyms would be an effective method of controlling to which information one has access. Typical user comments reflected the benefits of this interaction method, e.g. 'allows you to be anonymous, and to manage your exposure'.

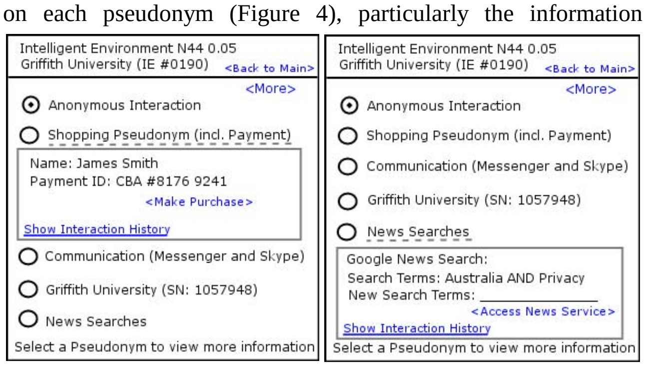

Figure 4. Example User Pseudonyms Interfaces

Users were then asked 'What type of feedback would you like to receive when interacting with an Intelligent Environment'. Responses indicated users were most interested in 'How collected information will be used' (89.9%) and 'What information is collected by the intelligent environment' (72.2%). These and other results are described in Table 1. The relatively high percentages of the responses suggest users are suspicious of data collection activities and want as much information as possible when evaluating privacy risks versus the rewards of using a service. Any developed intelligent environment architecture must provide users with this feedback in a timely, but non-distracting or onerous manner allowing them to judge risks to their privacy.

Table 1. Desired Intelligent Environment Interface Feedback

What type of feedback would you like to receive when interacting with an intelligent environment?	n = 18
How collected information will be used	88.9%
What information is collected by the environment	72.2%
Previous interactions you've had with this environment (or service).	61.1%
How long collected information will be stored before being deleted.	55.6%
A third party evaluation of the intelligent environment's reputation.	55.6%
Feedback on how to better interact with the environment (or service).	55.6%
Information on the owners and managers of the intelligent environment.	44.4%

The most popular services in the environment were location finding or direction services (13 users, 72%), local information (7 users, 39%), and public transport timetabling information (7 users, 39%). These services provide environmental information to users using a single interface, allowing the user to improve their awareness of their environment whilst controlling (or personalising) their exposure to potentially irrelevant information.

Participant's comments on the overall use of this ubicomp service infrastructure were positive. Users supported the improved access to community information and the internet, and the ability to communicate (and selectively share their location) with friends and family, but expressed privacy and security concerns regarding the use of ubicomp technologies and the sharing of personal information. This indicates the methods of securing users' information and maintaining the environment's security must be as transparent as possible to promote users confidence in this new method of information delivery.

6. DISCUSSION

This ubicomp infrastructure has the dual purpose of supporting community interaction in real third places, whilst providing hosting for localised virtual communities that form virtual third places. Community interaction is supported by providing a new interface to promote interaction with people in our local area.

Traditional and ubicomp communication and awareness tools can usefully be utilised to allow micro-communication and the coordination of meetings amongst existing social groups. This section discusses how the infrastructure accomplishes these goals, and examines how our ubicomp environment satisfies the requirements for effective virtual third places.

Our scenario briefly describes the interaction that occurs when a user enters an environment and accesses the ubicomp infrastructure. Users select a 'public face' that they wish to share with the environment, and this is passed to a central server to be shared with other users. The demographic information contained in the profile can then used to personalise users' display of the environment's other users. But the exchange of this information, and the user's personalisation preferences, can prompt privacy concerns amongst users. Our user study demonstrated wide-spread support for this service infrastructure, but highlighted the need for effective feedback on personal information collection and reuse.

To avoid sharing excessive amounts of information with the environment, the personalisation of the user display occurs on the users' handheld device. The demographic information provided to the environment (to facilitate sorting) should be sufficiently vague to prevent the recognising of the user across multiple (and potentially environmentally distributed) ubicomp environments. To further prevent user tracking, the public profiles selected by the user should not be stored in the environment or linked to any ubicomp service usage. This provides an anonymous infrastructure that users can use without fear of being tracked or of detailed profiles of the users activities becoming available to third parties. These environments will also be less effective if other privacy invasive or socially unpopular services are forced upon the user (e.g. directed marketing or pop-up ads) as these would turn people off interacting with the infrastructure.

Virtual communities provide neutral places away from work and home that allow playful conversation and interaction. But virtual communities are often frequented by a very specific user group, and lack the ability to promote interaction across a diverse community population. By providing access to these environments via ubicomp we effectively ground the virtual communities in real environments, and provide easy access to the greater community. The benefits of this can be examined by contrasting traditional and ubicomp access to virtual communities.

A virtual community set up to provide discussion on local issues is only effective as a third place if it examines local issues, and if it is accessed by a wide-range of community members. Virtual communities therefore must advertise their existence to community members, be easy to access (and visit regularly) and promote casual conversation that is free from politics or power. Traditional virtual communities have access problems, with the varying levels of computer literacy and access to the internet, and their lack of community localisation often reduces their relevance to the greater community and leads to unique knowledge-based power structures not conducive to relaxed, playful interaction.

Our virtual third places are accessed via common handheld devices from within our everyday environments. The existence of the environment is immediately obvious to anyone entering the environment, and this localised access ensures the entire community has the opportunity to interact with these virtual third places. Furthermore this localisation allows the rich context of the physical environment to interact with the virtual third place, and this promotes the sense of presence of these environments. Finally the anonymous interaction possibilities can lead to a sense of playfulness and casualness in the interactions that occur in these places. These factors make the virtual third place more accessible and relevant to the local community if served by a ubicomp environment.

7. CONCLUSIONS

This paper describes a ubicomp infrastructure that supports community interaction and social connectedness by providing local information, 'virtual community' interaction spaces and an awareness of users within the current environments. Through this infrastructure we can provide access to traditional communication and internet resources, promote the interaction between members of the community and provide anonymous access to ubicomp services. This provides support for the interactions that occur in physical third places, and provides a virtual environment for similar interaction between users. These virtual environments meet all the criteria for third place interaction identified by Oldenburg [1] and Soukup [12], and have the potential to form valuable third places for community interaction.

We expect these environments will eventually cover the majority of our cities, with smaller localised environment covering our homes, offices, transport networks and public areas. The extension of the city-wide wireless networks to provide local information and local interaction possibilities still provide the benefits of always-on internet access. These environments follow current projects that provide both free and (faster) subscription-based city-wide internet access to the public, e.g. Google-EarthLink's San Francisco wireless project [38]. As our handheld devices gain more processing power and we develop better wireless communication technologies we move towards always-on access to our friends, family and local community.

This infrastructure will be useful not only in suburban western cultures that are increasingly losing their 'third places' but in all cultures where social connectedness is declining. Future research should examine the use of ubicomp to localise and host virtual communities and examine the support of specific real third places (e.g. Coffee Shops, Clubs etc.). The types of virtual communities (e.g. Discussion Boards, Chatrooms, MUDs etc.) that will be effective in a given context will be dependent upon the characteristics and preferences of the local community. Of particular interest will be the implementation of this infrastructure en mass, allowing both the evolution of social practices and the adaptation of the technology to make use of this infrastructure in ways unimagined today.

8. ACKNOWLEDGMENTS

The authors would like to acknowledge the support of the Smart Internet Technology CRC.

9. REFERENCES

[1] Oldenburg, R., *The Great Good Place: Cafes, Coffee Shops, Bookstores, Bars, Hair Salons and Other Hangouts at the Heart of a Community*. 2nd ed. 1999, New York: Marlowe & Company.

[2] Watters, E., *Urban Tribes: Are Friends the New Family?* 2003, London: Bloomsbury.

[3] Wellman, B. *Little Boxes, Glocalization, and Networked Individualism*. in *Digital Cities II: Second Kyoto Workshop on Digital Cities*. 2002. Germany: Springer. p. 10-25.

[4] Coen, M.H. *Design Principles for Intelligent Environments*. in *Conference on Artificial Intelligent (AAAI-98)*. 1998.

[5] Carmichael, D.J., J. Kay, and B. Kummerfeld, *Consistent Modelling of Users, Devices and Sensors in a Ubiquitous Computing Environment.* User Modeling and User-Adapted Interaction, 2005. 15(3-4) August: p. 197-234.

[6] Kurkovsky, S. and K. Harihar, *Using ubiquitous computing in interactive mobile marketing.* Personal and Ubiquitous Computing, 2006. 10: p. 227-240.

[7] Myles, G., A. Friday, and N. Davies, *Preserving Privacy in Environments with Location-Based Applications.* IEEE Pervasive Computing, 2003. 2(1): p. 56-64.

[8] Iachello, G., et al. *Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service*. in *International Symposium on Ubiquitous Computing*. 2005. Tokyo, Japan.

[9] Hong, J. and J. Landay. *An Architecture for Privacy-Sensitive Ubiquitous Computing*. in *MobiSys*. 2004. Boston, Massachusetts, USA. p. 177-189.

[10] Schuler, D., *New Community Networks: Wired for Change*. 1996, New York: ACM Press.

[11] Kendall, L., *Hanging Out in the Virtual Pub: Masculinities and Relationships Online*. 2002, Berkeley, CA: University of California Press.

[12] Soukup, C., *Computer-mediated communication as a virtual third place: building Oldenburg's great good places on the world wide web.* New Media Society, 2006. 8(3): p. 421-440.

[13] Danet, B., *Cyberpl@y: Communicating Online*. 2001, Oxford: Berg.

[14] Keeble, L., *Why Create? A Critical Review of a Community Informatics Project.* Journal of Computer-Mediated Communication, 2003. 8(3).

[15] Liff, S. and F. Steward, *Community e-Gateways: Locating Networks and Learning for Social Inclusion.* Information, Communication & Society, 2001. 4(3): p. 317–40.

[16] Steuer, J., *Defining Virtual Reality: Dimensions Determining Telepresence*, in *Communication in the Age of Virtual Reality*, F. Biocca and M. Levy, Editors. 1995, Lawrence Erlbaum: Hillsdale, NJ. p. 33–56.

[17] Weiser, M., *Some Computer Science Issues in Ubiquitous Computing.* Comm. of the ACM, 1993. 36(7) July: p. 74-83.

[18] Jones, Q., S. Grandhi, L. Terveen, and S. Whittaker, *People-To-People-to-Geographical-Places: The P3 Framework for Location-Based Community Systems.* Journal of Computer Supported Cooperative Work, 2004. 13: p. 249-282.

[19] Campbell, R., J. Al-Muhtadi, P. Naldurg, G. Sampemane, and M.D. Mickunas. *Towards Security and Privacy for Pervasive Computing*. in *International Symposium on Software Security -- Theories and Systems*. 2002: Springer.

[20] Kummerfeld, B., A. Quigley, C. Johnson, and R. Hexel. *Merino: Towards an intelligent environment architecture for multi-granularity context description*. in *Workshop on User Modelling for Ubiquitous Computing*. 2003.

[21] Weiser, M., *The computer for the twenty-first century*, in *Scientific American*. 1991. p. 94-104.

[22] Griswold, W.G., et al., *ActiveCampus - Experiments in Community-Oriented Ubiquitous Computing.* IEEE Computer, 2004. 37(10) October: p. 73-81.

[23] Lahlou, S., M. Langheinrich, and C. Röcker, *Privacy and trust issues with invisible computers.* Communications of the ACM, 2005. 48(3) March: p. 59-60.

[24] Langheinrich, M. *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. in *International Symposium on Ubiquitous Computing*. 2001. Atlanta, USA. p. 273-291.

[25] Westin, A.F., *Privacy and Freedom*. 1967, New York: Antheneum.

[26] Chatfield, C. and J. Häkkilä. *Designing Intelligent Environments - User Perceptions on Information Sharing*. in *Asia-Pacific Conference on Computer-Human Interaction*. 2004. Rotorua, New Zealand. p. 570-574.

[27] Nguyen, D.H. and E.D. Mynatt, *Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems*, 2002, Technical Report, GIT-GVU0216.

[28] Chatfield, C., D.J. Carmichael, R. Hexel, J. Kay, and B. Kummerfeld. *Personalisation in Intelligent Environments: Managing the Information Flow*. in *Australasian Conference on Computer-Human Interaction*. 2005. Canberra, Australia.

[29] Langheinrich, M. *Privacy Invasions in Ubiquitous Computing*. in *International Symposium on Ubiquitous Computing - Privacy Workshop*. 2002. Göteborg, Sweden.

[30] Jiang, X., J. Hong, and J. Landay. *Approximate Information Flows: Socially-based Modelling of Privacy in Ubiquitous Computing*. in *International Symposium on Ubiquitous Computing*. 2002. Göteborg, Sweden. p. 176-193.

[31] Jendricke, U., M. Kreutzer, and A. Zugenmaier. *Mobile Identity Management*. in *Workshop on Security in Ubiquitous Computing, Ubicomp 2002*. 2002. Göteborg, Sweden.

[32] Berendt, B., O. Gunther, and S. Spiekermann, *Privacy in E-commerce: State Preferences vs. Actual Behavior.* Communications of the ACM, 2005. 48(4) April: p. 101-106.

[33] Lahlou, S. and F. Jegou, *European Disappearing Computer Privacy Design Guidelines v1.0.*, 2003, Disappearing Computer Initiative, Ambient Agoras Report, D15.4.

[34] Anastasi, R., et al. *Can You See Me Now? A Citywide Mixed-Reality Gaming Experience*. in *International Symposium on Ubiquitous Computing*. 2002. Göteborg, Sweden: Springer.

[35] Lederer, S., A.K. Dey, and J. Mankoff, *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments*, 2002, Technical Report, UCB-CSD-02-1188.

[36] Chatfield, C. and R. Hexel. *Privacy and Security within Intelligent Environments*. in *Australasian Conference on Computer-Human Interaction*. 2004. Wollongong, Australia.

[37] Hitchens, M., J. Kay, and B. Kummerfeld, *Secure identity management for pseudo-anonymous service access*, 2004, Technical Report 546. University of Sydney.

[38] Associated Press, 2006, Google-EarthLink selected for Wi-Fi project, 6 April, 2006, http://www.cnn.com/2006/TECH/internet/04/06/google.earthlink.wireless.ap/index.html, Last Accessed: 7 April 2006.

[39] Reid, D., 2005, Macedonia leads world with Wi-Fi, BBC News, http://news.bbc.co.uk/2/hi/programmes/click_online/4427960.stm, Last Accessed: 11 October 2007.