Context-awareness: Control over disclosure and privacy in a social environment

Varun Singh
Networking laboratory, Helsinki University of Technology
varun@netlab.tkk.fi

Abstract

Modern mobile phones in the near future will adapt their applications, services, and look-and-feel based on their usage and environment. This ability of the devices to adapt based on user's context provides new challenges in areas of context sharing, context management, and in the associated area of privacy. Inadequate relationship models make control over disclosure impossible, which manifests itself in either sharing too much information - compromising ones privacy, or sharing too little - constraining the use of context in a shared environment. In this paper, we define a new pseudo-hierarchical tag based relationship model to overcome the constraints of control over disclosure. Furthermore, we discuss some of the pitfalls of sharing context on user's privacy.

KEYWORDS: mobile, context-awareness, context-management, relationship model, privacy

1 Introduction

Pervasive mobile computing has become a reality, and with it, the need for intelligent devices has arisen. These devices would not only be self-configuring but also adapt services to their environment with little or no human interaction.

One can envision innumerable applications for these devices. For example, a device would easily adjust the screen's brightness and contrast using sensors that sense ambient light thus, enhancing usability. Another such application would automatically route data packets through a free Wireless LAN (WLAN) hotspot on detecting its availability instead of using the tariff-based 3G network. Furthermore, if a user is scheduled to be in a meeting the device can automatically route calls to a voice mailbox and announce to the caller when it would be more suitable to call the user, based on the user's schedule.

More innovative applications for example, adapting services based on remaining battery power. For instance, switching-off idle multimedia services when the battery falls below a pre-set threshold will provide extended talk-times to the user. Another more complex usage scenario wherein the device automatically on entering a supermarket fetches the user's shopping list and re-enumerates the list based on the supermarket's floor plans and the user's relative location to the items on the list.

However, it may be argued whether these actions should be carried out without the user's knowledge (automatically) or with limited user interaction. If a device shares its context with its peers then privacy related questions also arise, such as control over disclosure, and accountability of information.

In the paper we discuss about context-awareness in a social environment and try providing insight into: context-awareness and related taxonomy, uses of sharing one's context, and if sharing context influences someone else's decision making process. Furthermore, we discuss how privacy management can safeguard oneself from identity theft or awkward social interaction [2]. Figure 1 visualizes the areas related to context-awareness and describes the relationship between each entity in the system.

The paper is organized as follows: Section 2 introduces context, context-awareness and related terminology. Section 3 discusses device level context-awareness and Section 4 analyses scenarios for sharing context information and context management. Furthermore, Section 5 introduces privacy concerns for a user in such a shared environment. Section 6 briefly introduces existing relationship models available on the internet and we extend those to build a new relationship model to have better control over disclosure. Section 7 discusses vulnerabilities, security challenges and possible attacks using context-awareness. In Section 8 we conclude the paper by providing insight into possible future work.

2 Context

In this paper we use Dey's definition of context:

> "Context is a set of suitable environmental states and settings concerning a user, which are relevant for a situation sensitive application in the process of adapting the services and information offered to the user" [4].

2.1 Context-Awareness

Context-awareness is defined as: "the awareness of facts or circumstances that surround a situation (or a chain of) events"[1]. Furthermore, we should note that the *Environment* is not limited to the device's immediate surrounding but also includes the user's spatial and temporal attributes [10] such as to-do tasks (shopping, laundry), events (meeting, lunch, party), reminders etc [9].

[1] Dictionary.com

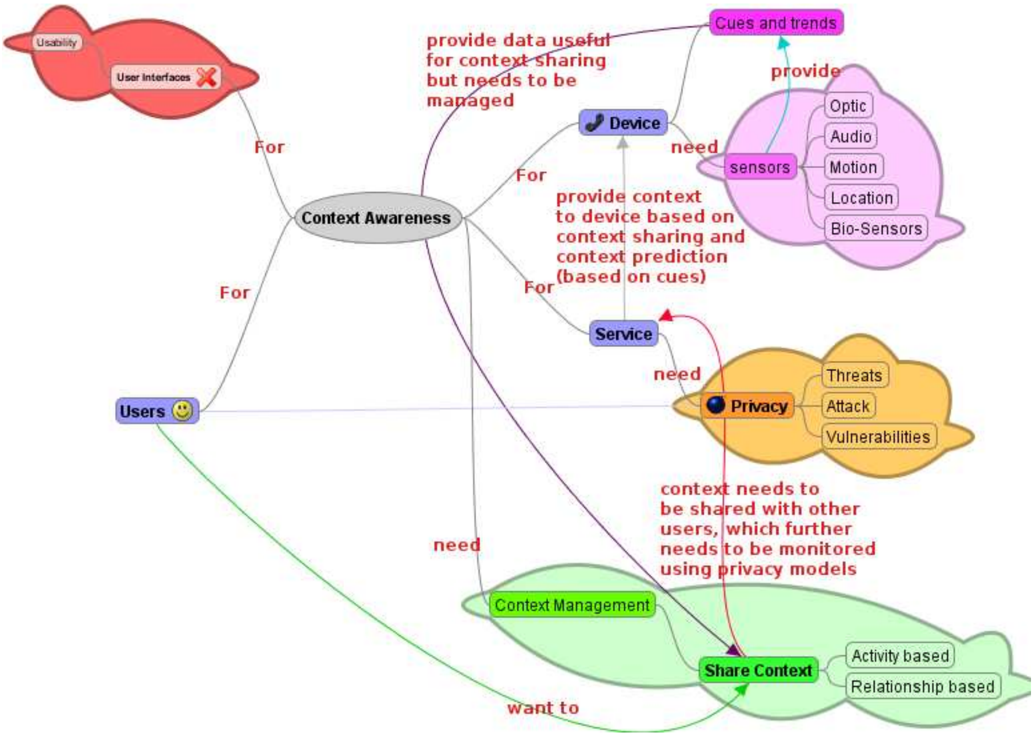
Usability
User Interfaces
For
provide data useful for context sharing but needs to be managed
Cues and trends
provide
Device
need
sensors
Optic
Audio
Motion
Location
Bio-Sensors
For
Context Awareness
provide context to device based on context sharing and context prediction (based on cues)
For
For
Service
need
Users
Privacy
Threats
Attack
Vulnerabilities
context needs to be shared with other users, which further needs to be monitored using privacy models
need
Context Management
Share Context
Activity based
Relationship based
want to

Figure 1: Mind map describing the relationship between the entities of context-awareness

A context-aware system also tries to build an understanding of other user's activity to provide context for its own activities [6]. We classify context-awareness as:

- **Device based**: context arising intrinsically from within the device and shared with applications running on the device.
- **Service based**: context is shared between devices of the same or different users.
- **Usability based**: context arising from human interaction or usage.

In the following sections, we begin with introducing device based context-awareness with the help of sensors and discuss possible applications. Furthermore, we introduce service based context-awareness using context-sharing.

3 Device

Simplest form of context-awareness information can be gathered by the device itself. By using sensors and other near field technologies like Bluetooth, WLAN or RFID etc the device can become aware of its ambient environment. This section of the paper looks at some of the currently available sensor technologies used in context-awareness and applications leveraging them. Furthermore, we define trends along with cues and patterns to help aid context prediction and awareness.

3.1 Sensor Technology

Modern mobile phones are equipped with many sensors. Those needed for context-awareness are listed below:

1. **Optic**: Camera, photo diode etc. for example can be used to gauge the light intensity in the user's environment and adapt UI or display-related aspects.
2. **Audio**: Microphone etc can detect ambient noise to adapt the loudspeaker's setting, additionally provide echo or noise cancellation, or change codec parameters for an ongoing call (based on call quality) etc.
3. **Motion**: Accelerometers etc can help gauge motion. For example, the phone might turn-off Bluetooth service when moving quickly, to reduce power consumption or automatically change display orientation (landscape or portrait mode, to aid usability) etc.
4. **Location**: GPS to provide reliable location data, Bluetooth/WLAN to detect proximity or a combination of the above technologies to provide more pertinent user context.
5. **Bio-sensors**: Heartbeat sensor etc. For example can be used for wellness applications or workout based applications like varying the tempo of the music based on heart pulse or motion during workout.

The above sensors provide localized (i.e. immediate surroundings of the user) data to the device to gauge its current context. By combining multi-sensor data more complex contexts or scenarios can be envisaged.

3.2 Context-Prediction using Sensory Cues, Patterns and Trends

Devices can predict context using sensor data and spatio-temporal knowledge from other applications. In this sec-

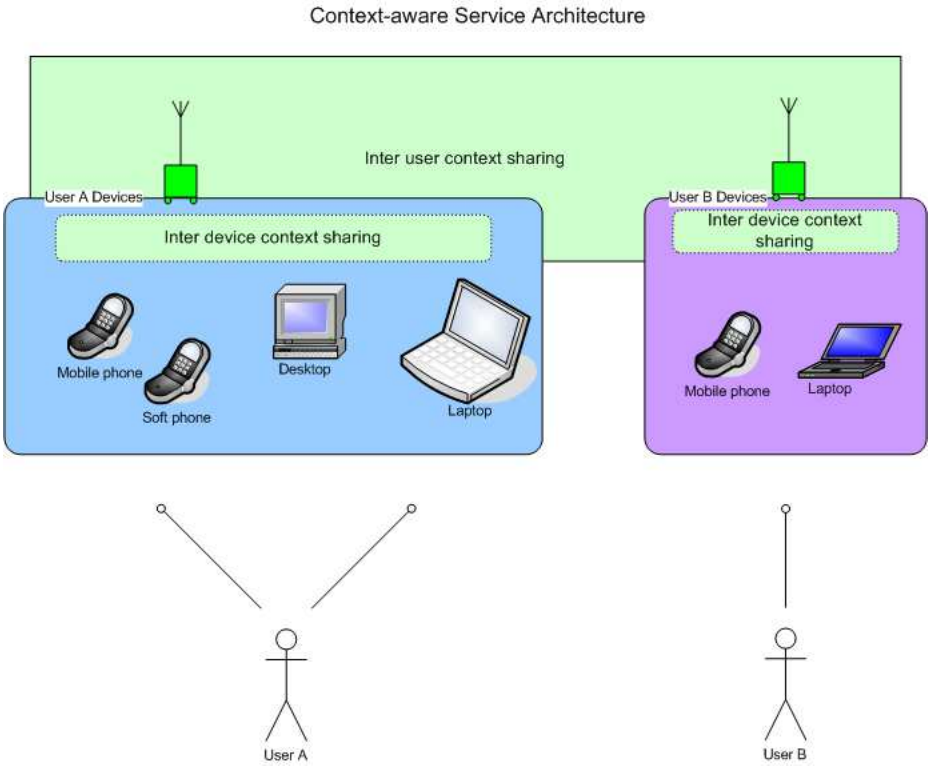
Context-aware Service Architecture
Inter user context sharing
User A Devices
Inter device context sharing
Mobile phone
Soft phone
Desktop
Laptop
User B Devices
Inter device context sharing
Mobile phone
Laptop
User A
User B

Figure 2: Context-awareness service architecture showing inter-device context sharing and peer-level (inter-user) context sharing

tion we discuss the uses of sensory cues, event patterns and trends.

Cues are sensor thresholds that provide pertinent information to help the applications predict context. By defining cues, sensors are able to abstract physical data values into pseudo-logical ones. Using multiple cues from the same or different sensors, applications are able to predict context even more accurately [16]. Devices can also detect repetitive actions as *patterns* like, daily chores, periodic meetings etc.

To further help with context-prediction, we define *trends*, these are psuedo-perodic events and are detected by the trail of events preceding it. That is, if the sequence of events matches with a previously defined context change or if the sequence of events do not change significantly then such trends can be detected with high probability.

Therefore, cues, shared cues (from other users), patterns and trends make context prediction more efficient.

3.3 Application based classifications of context-awareness

Schmidt et al. [16] have extensively classified parameters for context-awareness. However, we find it more useful to classify them based on the application's ability to leverage context-awareness. They are as follows:

1. **Adaptive User Interfaces**

   (a) based on mode of operation, interaction styles. For example, adapt display modes based on ambient light.

2. **Context-Aware Communication**

   (a) **QoS and Cost** are driving forces: for example switching to 3G data services from WLAN due to QoS or mobility reasons and vice-versa for monetary reasons.

   (b) **User's location**: absolute or relative position or co-location can trigger or provide opportunity of communication.

   (c) **Callee's**[2] **context**: shared context such as signal strength, meeting calendar, battery power etc.

3. **Proactive Application Scheduling**

   (a) Power based: Adaptive battery thresholds for powering off idle applications can be set to better conserve battery power.

   (b) Activity based: turn off idle applications or store application-state in memory (FLASH or MMC/HDD etc) for quicker access.

Based on the above applications we introduce context-sharing as service based context-awareness.

4 Context-sharing as a service-based context-awareness

In Figure 2 we classify context-awareness services; it follows a two-tiered architecture. In the first-tier user's devices share context: *inter-device context-sharing*. In the second-tier the context is shared between users: *inter-user context-sharing*. An example for inter-device service is, an incoming

[2] The person being called by the caller

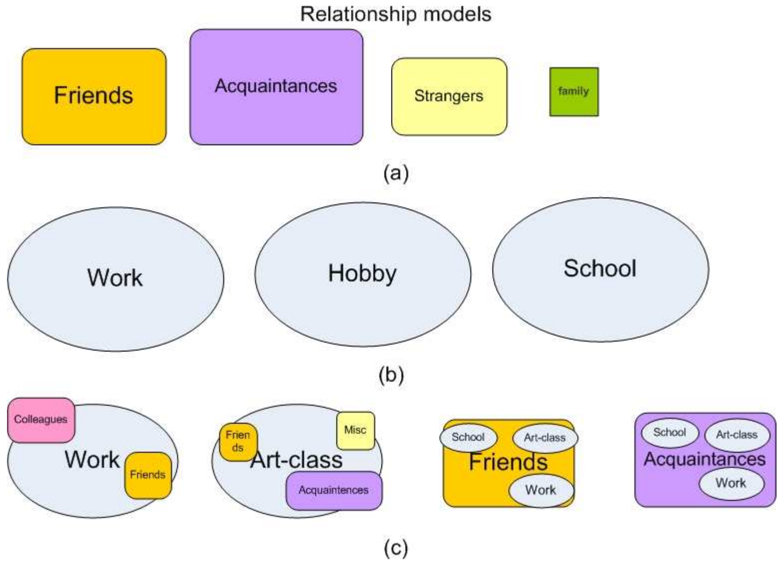

Figure 3: Venn diagram based relationship model with an intuitive GUI. (a)User relationship model like Orkut, Flickr (b)Activity based relationship model like LinkedIn, Facebook etc (c)New multi-label relationship model with subsets for better control over disclosure.

call is routed to the current active device and not necessarily to the number that was called (in VoIP there exist SIP extensions to implement the same). Another example would be the seamless migration of user's sessions (instant messaging, web-browsing etc) between different devices (mobile phone, laptop, desktop etc). On the other hand, context-aware communication defined in the previous section (Sec. 3.3) is a good example of inter-user context-sharing.

Currently, most of the work done in the area of context-sharing for mobile devices has been from a technical standpoint and very few implementations exist. Those that do are typically, research projects such as presence or location sharing in phonebook contacts [13, 1], calendar to-do/notes, or reminder information [5] wherein shared data (as defined earlier in context-aware communication) is used to determine relevant context of users in a closed group. The architecture should allow any pertinent data to be shared as context between users.

Based on the classification provide by Petersen et al. [10] and Schmidt et al. [16] we re-enumerate factors pertinent to context-awareness in a social environment:

1. **User's activity**: based on life patterns (generic daily-schedule or repetitive schedules like, weekly beer-drinking with college buddies), emotional state, and spatio-temporal activities (such as reminders, to-do, events etc).

2. **User's Social Environment**: based on proximity to others, social interaction, relationships etc.

3. **Infrastructure**: based on availability to computing, communication resources etc.

While infrastructure context sharing appears non-intuitive, research [13] shows that battery and network signal strength of the callee's device can play an important role in the caller's decision making process to make the call. We can conclude that from a context-sharing perspective, device and service contexts are most useful for context-prediction and that usability is a data presentation challenge and should be tackled separately. Furthermore, sharing of context between peers or other users is non-trivial and requires control over disclosure with a dynamically changing group and complex privacy models.

5 Privacy in context-awareness

Similar to the two-tier classification of context, privacy also defines two levels; inter-device privacy and inter-user or peer level privacy. The first level, inter-device privacy is trivial and can use symmetric encryption keys to protect the context data. However, the latter case of peer level privacy is more complex and for the rest of the paper, the word privacy refers to the inter-user privacy unless stated otherwise.

Since we do not live in a utopian world, privacy is an important aspect of security in social networks. Privacy controls the relationship boundary between individuals, individuals and organizations, and individual and the general public [15]. Furthermore, everyone maintains a different identity called *relational self* [17] for each of their many relationships, sharing and hiding a different bit of themselves from everyone.

We may continually find ourselves in social situations where we do not wish to share our context information with everyone, but with a subset of people we are acquainted with. However, this subset maybe very dynamic and be very situation-specific. This poses an interesting human interaction problem of classification of a dynamic group of people.

Situations may arise where people either disclose too much or too little information, thus rendering the system ineffective. Therefore to have control over disclosure a need for relationship model arises. In the next section, we discuss existing relationship models and introduce a new representation model.

Currently, in the mobile environment one finds fewer strangers in their phonebooks than when compared to their contact lists on web based social networks [3]. However, this will soon change when services will converge and data is made accessible across services and applications.

More information does not necessarily provide better context, fuzzy information is sometimes good enough to describe a context. For example, by sharing the busy and free data of one's calendar is sufficient knowledge for a caller to decide if he should call the person or not, instead of knowing the specific details of the calendar entries [14]. even in the case of location-based context, users don't require accurate location data, even relative location information is quite useful in context-based decision making process [11], for example, *at work*, *not at home*, *out for lunch* or even plain *busy*.

6 Relationship Representation models

With the appearance of social networking sites, users continually find themselves arranging their contacts based on parameters described by the service. For instance, Orkut (Google's social networking site) [12] allows users to arrange their contacts on the basis of their relationship which ranges from *haven't met* to *acquaintance* to *friends* to *best friends* (Fig. 3(a) describes a visualization of such a model). Their relationship representation doesn't take into account family relationships but allows customized groups which can be self-configured by the user. However, Orkut's privacy management only makes a distinction between the user's contact list (they may be strangers or best friends - it doesn't matter, they are considered the same for privacy related issues) and those not on the user's contact list. So, there is no granularity of control over disclosure with-in the contact list.

Flickr (Yahoo's photo-sharing website) [8] on the other hand allows only 2 levels of contacts namely, namely *family*, *friends* and general public. However, Flickr's design allows family and friends can be mutually exclusive or inclusive). This allows for a granular control over disclosure (picture sharing) between known and unknown people. However, doesn't allow disclosure to a sub-group of people.

Facebook [7] on the other hand allows complex relationship representation. Contacts can be represented by multiple relationships based on hobbies, activities, or relationships (Fig. 3(b) visualizes such a model). However, Facebook doesn't use these groups for privacy control. Instead, it relies on user-defined groups or networks (like, school, place of work, city etc) for privacy control.

We attempt to build a new relationship model which takes into account some of the above scenarios. Instead of representing friends by *activity* (art-class, camping, salsa, summer job, MMORPG[3]) or *relationship* (acquaintances, friends, met-randomly, strangers, colleagues, best friends, relatives) instead arrange them in cliques and to each clique assign a relationship attribute or tag (one or more, as the situation maybe).

A clique is literally defined as "a narrow exclusive circle or group of persons; especially: one held together by common interests, views, or purposes"[4]. A person might belong to multiple cliques and thus be analogous to a multiple-label representation (psuedo-hierarchical, tag based relationship model) instead of a folder based hierarchical model (Fig. 3(c) describes two examples of such a visualization). It is called psuedo-hierarchical because of the representation i.e. a set may exist inside another set but is not limited to just one set. For example, friends may exist under multiple groups.

Visualization is a human interaction challenge; therefore we make use of basic Venn diagrams to visualize groups. From concepts of set theory and employing touch screen graphics, we are able to represent and target a person or specific group in an intuitive way. For example, if a user wants to share his forthcoming movie plans with a closed group friends like, friends from the summer-job and acquaintances and friends from the art-class (See Fig. 4) or organize a party with his co-workers (See Fig. 5). It should be easy to logically or intuitively target them.

$$\{(\textbf{acquaintances} \cup \textbf{friends}) \cap \textbf{art-class}\} \cup \{\textbf{friends} \cap \textbf{summer-job}\}$$

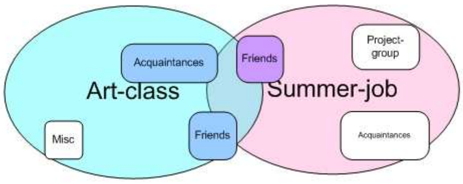

Figure 4: Example of textual and graphical representation of the multi-relationship representation model: *movie plans with friends from the summer job and acquaintances and friends from the art-class.*

$$\{\textbf{friends} \cap \textbf{work}\}$$

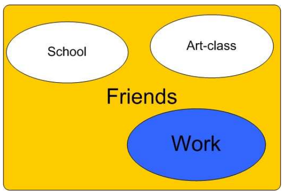

Figure 5: Another example of textual and graphical representation of the multi-relationship representation model: *party with friends at work.*

7 Vulnerabilities, Threats and Attacks due to context-awareness

We use Raento et al. [15] parameters of privacy management to define some of the vulnerabilities and threats of sharing context. Parameters defined by them for assessment are:

[3] Massively Multiplayer Online Role-Playing Game

[4] Merriam-Webster.com

- **Control**: Type and depth of information revealed to peers, it is dynamic and situation-specific. User should be aware of the risk of improper disclosure.

- **Reciprocity**: It helps build trust since trust works both ways i.e. information shared with should be equal between peers. For example, if one user shares his location information then other users that access this shared context should also share their location, to maintain equal information sharing.

  Degree of reciprocity is the amount of information that is shared in a context. Some contexts like for example location can provide a lot of detail like exact location (HUT-Computer Science building, Kamppi Shopping center etc) or fuzzy information like (Otaniemi, Ruoholahti etc). Either a decentralized system or a complex handshaking protocol is needed for context-sharing to maintain the same degree of reciprocity.

- **Accountability**: The users should be able to retrieve which other users accessed their shared-context.

- **Plausible Deniability**: allows users to customize their context data, in situations when the users wish to hide or fake their context to a person, a group or a subset of people.

Context-faking instead of hiding their context, users provide incorrect context for a short period of time. *Context-spoofing* when some users provide incorrect context to gain access to other users' context (due to rules of reciprocity).

At first glance, both context-faking and context-spoofing appear similar. However, the difference lies in purpose. In context-faking users hide their context which might mislead other users however, in context-spoofing users exploit the system to gain personal information about other users. User studies have shown that plausible deniability is an important parameter in privacy and cannot be done away with [15].

Online-stalking is an important vulnerability of context-sharing. Despite plausible deniability, shared context in many scenarios is valid. Moreover, if context is broadcasted (e.g. IM status messages, Twitter/Facebook status messages etc.), accountability is difficult to ascertain. So the shared context should be explicitly requested from the other user but it should not require an explicit human interaction for the response however the request and the response should be archived for latter inspection, if need be. This will deter or prevent *online-stalking*

Impersonation in the mobile scenarios is limited due to usage of devices which have unique identifiers like IMEI numbers, phone numbers, SIM card authentication etc. However, spoofing of these identifiers is possible by methods such as device cloning etc. These kinds of attacks can lead to digital stalking. Furthermore, theft of a mobile device might lead to further aggravation of this situation.

Therefore, from the above scenarios *trust* appears to be an important parameter for privacy. We believe that trust has to be situation specific and session limited. However, reactive trust is infeasible in virtual environments as it requires continual user interaction. It might be further contemplated if trust should be contractual. If so, trust needs a period of validity and should be set by the user sharing the context and constraint by laws of reciprocity and therefore can be terminated by either user.

8 Conclusion and Future Work

We conclude from our research that for context-sharing to succeed, the user must be aware of the risk of sharing context with unintended users. Therefore control over disclosure is important. Furthermore, context sharing cannot be passive or reactive as it would require constant user interaction (i.e. when peers query for user's context). However, accountability is important and the user should be able to see which peers queried for his shared context.

To overcome some of the problems with disclosure we introduced a new multi-label tag based relationship model. Using intuitive user interfaces and representation the model allows subset selection. This allows better control over disclosure. One major pitfall of this relationship model is that it presumes the pre-existence of the relationships (links, labels, tags etc.) in the model. Therefore the success of the model totally rests on the user's commitment on maintaining it, as is the case with other relationship models.

Future work may involve dynamic generation of groups based on spatio-temporal activities and innovative a two-way verification method to auto-generate these groups. Furthermore, system will require a probabilistic end-to-end trust system to ascertain validity of context.

References

[1] H. G. A Schmidt, T Stuhr. Context-phonebook - extending mobile phone applications with context. In *Third Mobile HCI Workshop*, 2001.

[2] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 357–366, New York, NY, USA, 2007. ACM.

[3] J. Breslin and S. Decker. The future of social networks on the internet: The need for semantics. *Internet Computing, IEEE*, 11(6):86–90, Nov.-Dec. 2007.

[4] A. K. Dey. Understanding and using context. *Personal Ubiquitous Comput.*, 5(1):4–7, 2001.

[5] A. K. Dey and G. D. Abowd. Cybreminder: A context-aware system for supporting reminders. In *HUC '00: Proceedings of the 2nd international symposium on Handheld and Ubiquitous Computing*, pages 172–186, London, UK, 2000. Springer-Verlag.

[6] P. Dourish and V. Bellotti. Awareness and coordination in shared workspaces. In *CSCW '92: Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 107–114, New York, NY, USA, 1992. ACM.

[7] Facebook. http://www.facebook.com, accessed 15-March-2008.

[8] Flickr. Yahoo's social aware photo sharing site, http://www.flickr.com, accessed 15-March-2008.

[9] J. Hakkila and J. Mantyjarvi. Collaboration in context-aware mobile phone applications. In *HICSS '05: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 1*, page 33.1, Washington, DC, USA, 2005. IEEE Computer Society.

[10] A. Kofod-Petersen and J. Cassens. Activity Theory and Contex-Awareness. In S. Schulz, D. B. Leake, and T. Roth-Berghofer, editors, *IJCAI-05 Workshop on Modelling and Retrieval of Context – Working Notes*, pages 1–12, Edinburgh, 2005. IJCAI.

[11] K. Laasonen, M. Raento, and H. Toivonen. Adaptive on-device location recognition. In *Pervasive*, pages 287–304, 2004.

[12] Orkut. Google's social networking site, http://www.orkut.com, accessed 15-March-2008.

[13] A. Oulasvirta, M. Raento, and S. Tiitta. Contextcontacts: re-designing smartphone's contact book to support mobile awareness and collaboration. In *MobileHCI '05: Proceedings of the 7th international conference on Human computer interaction with mobile devices & services*, pages 167–174, New York, NY, USA, 2005. ACM.

[14] L. Palen. Social, individual and technological issues for groupware calendar systems. In *CHI '99: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 17–24, New York, NY, USA, 1999. ACM.

[15] M. Raento and A. Oulasvirta. Privacy management for social awareness applications. In *CAPS '05: Proceedings of the workshop on Context Awareness for Proactive Systems*, pages 105–114, 2005.

[16] A. Schmidt, M. Beigl, and H.-W. Gellersen. There is more to context than location. *Computers and Graphics*, 23(6):893–901, 1999.

[17] I. R. S.M. Andersen and N. Glassman. The unconscious relational self. In J. U. R. Hassin and J. Bargh, editors, *The new unconscious*, pages 421–481, New York, 2005. Oxford University Press.