Trust-centered Design for Multi-Display Applications

Ekaterina Kurdyukova
University of Augsburg
Universitaetsstr.6a
86158 Augsburg
Kurdyukova@informatik.uni-ausburg.de

Elisabeth André
University of Augsburg
Universitaetsstr.6a
86158 Augsburg
Andre@informatik.uni-ausburg.de

Karin Leichtenstern
University of Augsburg
Universitaetsstr.6a
86158 Augsburg
Leichtenstern@informatik.uni-ausburg.de

ABSTRACT
This work describes a trust-centered user study that was conducted during the design process of a multi-display ubiquitous application. The objective of the study was to find out how the adaptation of the displays should be designed in order to protect user trust. The study was conducted in the form of focus group interviews; it investigated user attitude towards data and events that can be seen as trust-critical in a multi-display interaction scenario. The quantitative results, along with user comments and discussions, provide an interesting insight how the system should be adapted in order to preserve user trust.

Categories and Subject Descriptors
H.5.2 [**User Interfaces**]: Evaluation/methodology, User-centered design

General Terms
Design, Experimentation, Human Factors.

Keywords
Trust aspects, adaptive displays.

1. INTRODUCTION
Multiple display environments are deeper and deeper integrated in the modern life. The environments including large public displays and small private devices offer users certain benefits. For instance, they help us to profit by personalization of the displayed data: advertising in shopping malls, routing directions, personal schedules can unobtrusively provide fast access to needed data. Such content adaptation intelligently adjusts the display to the current situation, user profile, or the surrounding context.

However, apart from numerous benefits, content adaptation may also harm the user. Automatic content adjustment can lead to the disclosure of private data on public, as well as to unexpected and undesired system behavior. Unexpected system behavior and disclosure of personal data may leave user with a feeling of losing control over the situation, discomfort, and as a possible result: destruction of user trust. Having such negative experience, users may refuse to use the system at all in the future. Therefore, the trust-sensitivity of data and events should be carefully investigated when designing a new system.

The user-centered design is known to be an efficient approach for the design of interactive applications. User involvement in every stage of the design process guarantees the optimal fulfillment of user needs and requirements. In this paper, we show how user-centered design can be applied in a trust-centered study.

2. TRUST-CENTERED USER STUDIES
Trust-centered user studies have shown to be an efficient approach to understand user attitude towards trust-critical design aspects. For example, Roecker and colleagues [10] conduct a trust study at the evaluation stage of the design process. Users were asked to evaluate the design concept in terms of trust protection and to compare it with other less trust-protective systems. The main goal of the study was to understand which situations users find appropriate for content personalization on public displays.

Another trust-related study was conducted by Graham and Cheverst [3]. The study investigates the problem of mapping in context-aware mobile applications. Mapping issues often negatively affect the interaction process and thus tend to diminish user trust. Based on the evaluations of two mobile guides, the authors found six characteristics of mapping problems that should be carefully attended by interaction designers: determinism, transparency, accuracy, indexicality, predictability of content, and predictability of behaviour. Although the work significantly contributes to the design guidelines for trustworthiness, it solely concentrates on the mapping problem in mobile usage scenarios.

The study presented in our paper investigates trust-critical aspects in a multi-display scenario. In contrast to the above mentioned works, our study focuses on the problems that are typical for a multi-display environment: privacy issues, automatic adaptation of the content, and system failures. It aims to analyze which data and events users see as trust-critical, and thus how the system adaptation should be designed. Here under the notion of trust we understand users' readiness to confide to the system their private data, and consequently users' expectation that the system treats the data in a confident way.

As the basis for the study, we took example applications for University multi-display system. The system is supposed to run on public displays situated in floors and on private mobile displays belonging to the students.

The trust-centered study was conducted in the form of focus group interviews. Compared with individual interviews, focus groups encourage research participants to a collaborative discussion. Such discussion enabled us to acquire a better understanding of user perspectives and attitudes towards trust problems.

After an overview of the data and events that can be seen as potentially trust-critical, we describe the focus groups study. We elaborate on user attitudes towards trust-critical data and events when interacting with University displays. The quantitative rankings of data items and events are illustrated by discussions and comments of study participants.

3. TRUST-CRITICAL DATA AND EVENTS

Below we describe the data usually displayed on public screens which can be regarded as potentially trust-critical. Then we discuss the potentially trust-critical events that may occur when interacting with multiple displays.

3.1.1 Personal Data on Public Displays

Most of the research devoted to trust issues discuss the disclosure of private data on public as the main reason for the loss of trust. This private data may be classified as following:

Personal data, referring to the data directly related to the user. For example, the name of the user, check-in details at the airport, or a *personalized view of an application*. Vogel et al. [14] present a proximity-based public display that visualizes personal schedules. Roecker et al. [10] designed a public display to browse personal emails or view personal documents.

Personal data of other people. This data basically repeats the category described above, but refers to the details belonging to other people. For example, the visualization of a user's social network or the list of a user's contacts.

User preferences. This category is frequently used in adaptive systems in order to adjust the content to a concrete user model. Here the personal data of the user is not directly visualized on the public screen. Instead, the knowledge of the user model is used to efficiently adapt the screen content. For example, Villar et al. [13] adjust the display content based on the user preferences saved on a wearable device.

Navigation info. A route, an immediate direction, or a destination can be displayed on a public screen. For example, Rukzio et al. [11] introduced a public display showing the user the right direction on street crossings. Kray et al. [5] developed a multi-display system for indoor navigation. In both systems the immediate user direction is observable by the by-standing public.

Body-related data. Research projects and commercial solutions often place body-related user data on public screens. For instance, bio data of the user, such as heart rate, motion data, such as speed, can be used to control fitness games [6, 7]. The achievements and the progress of the user are shown on a large screen which can be seen by others. The observation in this case may be seen negatively: as a pressure or as a disclosure of private data. However, the observation may also have a positive impact, as a motivating and inciting factor. Polar [9] offers a commercial multi-display solution for gyms where sportsmen can trace their performance during a collective exercise. A large screen enables them to compare their results with those of others, raise team spirit, or inspire for competition.

3.1.2 Events Potentially Impacting Trust

Based on the literature overview that considers trust aspects from various perspectives [2, 10, 12], we can classify the aspects that negatively influence user trust as follows:

Automatic adaptation implies adjustment of content or system behavior based on some predefined rules. If the user is not aware of the rules in advance, surprising and unexpected system behavior potentially leads to user frustration and losing the sense of control.

System failure. If the system does not execute a task in an expected manner, and the user interface is not able to react appropriately, the user tends to be frustrated and to feel a lack of feedback.

Privacy issues, disclosure of private data. This category covers the most typical issues in the case of interaction with public displays. The personalized content on a public screen may be observed by by-standers and co-interactors.

4. FOCUS GROUP STUDY

In order to find out what users would appreciate to see and to hide on a public screen, when and how user interface can be adapted, we conducted a trust-centered focus group study. Six university students participated in the study, all from the Computer Science faculty, male and aged between 23 and 26. Although all the participants belonged to the same user group, IT students, they did represent the most probable users of our display applications. Since the display was installed in a floor of IT faculty, the most of our potential users were expected to be IT students.

During the study we have shown the participants various prototypes on a large public screen installed in a university room. The prototypes simulated scenarios of two applications designed for the university multi-display system: Friend Finder and Media Wall. Both applications were designed in a user-centered way; the prototypes were built based on collected user requirements and intermediate feedback.

Friend Finder is an interactive campus map that shows the current location and status of user's friends. Since many students have difficulties in orientation on campus (especially in new buildings), Friend Finder also supports the routing function, showing a detailed path to a selected friend. As an extension of the routing function, we designed an application on a mobile projector that supports immediate navigation. Users could switch the views on the mobile projector: the overview map with self-updating user position, and an arrow view pointing to the current direction. Media Wall application represents the gallery of media items (pictures or videos) uploaded by students or scientific staff. Users can rank the media items, upload new items, and view their favorite ones.

Each scenario was presented by the moderator, in Wizard-of-Oz style, as a screen flow. The scenarios demonstrated the screens containing private data, or illustrating some events. After each demonstration the participants were asked to evaluate the presented data and events on a scale from 1 to 5 (1 as "not trust-critical" and 5 as "very trust-critical"). Although such evaluation can be considered rather simplistic, it gives a clear cue about users feeling of their trust to the system. The students were asked to comment on their rankings and discuss trust issues in the current scenario. If a trust problem was identified, we also discussed possible solutions. Although the prototypes illustrated only the

public display application, the study participants were encouraged to think about solutions involving mobile displays as well.

Below we summarize the results, discussing first our findings on trust-critical data, and then the findings regarding trust-critical events.

4.1 Trust-critical Data

Bearing in mind the findings on potentially trust-critical data (section 3), we designed the prototypes so that they cover most of the data categories that are usually exposed on public. Although our university applications didn't involve any body-related data, the prototypes included the remaining categories. *Personal data* reflected the user name and the authorship of pictures on Media Wall. *Personalized application view* and *data belonging to other users* referred to the visualization of user's social network in Friend Finder. The route and the arrow displayed during navigation also refer to the *personalized view*. User *preferences* related to the personalized favourites on Media Wall.

After a short summary of students' rankings given in the table 1, we elaborate on user attitudes towards presented data.

Table 1. User trust-rankings of displayed data items

Data Category	Mean	St. Dev.
Personal Data: Name	3,17	1,17
Personal Data: Authorship	1,67	0,82
Preferences: Media Favourites	2,83	0,75
Personal Data of Friends: Names	3	0
Personal Data of Friends: Pictures	2	0,63
Personal Data of Friends: Availability	2,17	0,75
Personal Data of Friends: Locations	3,83	0,75
Map: Route and Final Destination	1,67	0,82
Navigating arrow: Direction	1,5	0,55

Personal data. User name shown, for example, on the welcoming screen of a public display was perceived as a slightly trust-critical item (M: 3,17; D:1,17). However, participants commented that in university environment the name is not extremely confident information: an interested person can find it out from common peers, colleagues, etc. Moreover, the students see the name as public data anyways "*You just have to wait until someone calls me, and you'll find out my name*". Although the students could not imagine any malicious situation where their name could be misused, they nevertheless preferred to leave only the first name on the screen. In a more public environment, such as a street or a shopping mall, the full name exposition would be perceived as much more trust-critical.

The prototype of Media Wall application showed author names attached to every media item. Therefore, if the user name is displayed on the screen, an observer could immediately see which media the user is authoring. The explicit authorship however was not perceived as trust-critical (M: 1,67; D:0,82). On the contrary, the participants would appreciate to expose their authorship: "*If I publish my pictures on the display, I do want other people to see them… and to see that the works are mine!*" The situation changes however if the user's media have low rankings: the fact of unsuccessful creativity is preferred to be hidden.

Preferences. Media Wall personalized the screen content by showing user's favorites. The study participants generally did not find the exposition of these preferences as trust-critical (M: 2,83; D: 0,75). However, the presence and the selection of favorites should be controllable: the content of these media can negatively impact user's image in public eyes. For example, if the screen shows some aggressive media associated with the user profile, it can confuse the user. A similar situation can be observed in a non-university setting: for instance, a public screen that starts to advertise diabetes pills for the user can be found embarrassing and intrusive.

Personal data of others, personalized application view. Friend Finder application visualized social network of the user overlaid on the campus map. It showed the friends that are currently located on the campus, their availability (red frame for 'busy', green frame for 'free'), and portraits (see Figure 1).

According to the rules of the social networks, all the data was controlled by the friends and was published on their free will.

Surprisingly, the majority of friends' personal data was not found trust-critical for a public observation: the portrait pictures (M: 2; D: 0,63) and availability (M: 2,17; D: 0,75) in opinion of the participants can be observed by everyone. The pictures without names were seen to carry no private information: "*If someone knows a person at the picture, he will know her name as well. If you don't know the person in face, what will you know from the picture*?"

We also offered the students a view containing additionally the full names of their friends. The names were found slightly trust-critical (M: 3, D:0). However, their presence was seen useless: they double the information on the pictures.

Surprisingly, disclosure of friends' locations was rated higher than other data items (M: 3,83, D: 0,75). Since the public screen may be observed by instructors and professors, some issues may arise if the displayed peers stay in unintended place (for example, during the lecture). The students do want to open the fact of their presence on the campus, but not as granular as the room or the part of the building. The best solution for such interface would be to control the granularity of location. According to the social environment around the display, the user can quickly change the locations view from detailed (room, building part) to general (building, campus).

Destination, route, and direction. Using Friend Finder application, a user could get the route to a selected friend and further be navigated by means of personal projector. Neither route, nor the destination were found trust-critical (M:1,67; D:0,82). The only sensitive moment in the "getting the route" scenario was seen by the indirect disclosure of private intention: to meet a certain person. However, the study participants saw it less critical in university context. The navigation arrow supported by a mobile projector was also not found trust-critical (M: 1,5; D:0,55): "*If someone is interested where I will go next, he will anyway see it in a second!*"

All in all, the degree to which personal data can be disclosed depends on the application context. At a university the exposure of personal data is seen less privacy-critical. However, in a more public environment like the street or a shopping mall, the degree

of privacy would be higher, and thus more data should be hidden. The users' attitude towards the disclosure of personal data of others follows the rules of the social networks: if the peers open their data, they are aware that the data may appear on a public display.

4.2 Trust-critical Events

In the second part of the focus group study we went through scenarios that simulated potentially trust-critical events: system failure, privacy-critical events, and system adaptation. Important to notice that the latter usually assists the first two events: the system is adapted to mask or repair the system failure, or to protect privacy. Therefore, we did not show any scenarios for pure adaptation; instead the adaptation happened in combination with privacy-critical events and system failures. All in all, 20 scenarios were shown and discussed with the study participants. Table 2 summarizes the presented scenarios and respective user rankings.

Table 2. User rankings of demonstrated events: System failures (SF) and privacy-critical events (PR)

Nr	Scenario description	Mean	St. Dev.
	User gets a route to a selected friend		
1	The selected friend suddenly changes position (SF)	3,17	0,41
2	The selected friend suddenly disappears (SF)	2,83	0,41
3	The route is suddenly drawn to a wrong person (SF)	5	0
4	User explores his friends on the public screen. A stranger explicitly observes the user (PR)	3,83	0,75
	A stranger co-interacts with the display, retrieving there his social network		
5	All friends of the user remain on the screen unmasked (PR)	4,17	0,41
6	Only common friends of the user and the stranger remain on the screen (PR)	1,83	0,41
7	All friends of both users are shown on the screen, but masked (PR)	1,33	0,52
	User ranks a selected picture on the display		
8	A stranger explicitly observes the user (PR)	3,5	1,38
9	Wrong ranking is submitted (SF)	4,33	0,52
	User uploads a photo to the public screen		
10	Preview with a right photo is shown. But a wrong photo finally uploaded (SF)	4,8	0,45
11	A wrong photo is uploaded (without preview) (SF)	5	0
12	The right photo is uploaded, but in a wrong orientation (SF)	5	0
13-15	Repeat scenarios 1-3, but on mobile projector (SF)	No differences to pub. display rankings	
16-18	Repeat scenarios 10-12, but on mobile projector (SF)		
	Navigation with mobile projector. Switching between map and arrow view		
19	Suddenly only arrow view is available, no map view (SF)	4,4	0,55
20	Arrow points to an unrealistic direction (wall or ceiling) (SF)	4,4	0,55

In order to summarize the attitudes of participants towards the presented scenarios, below we describe some observed trends.

People tend to justify a system failure, if the visualization is plausible. The first interesting trend we have noticed related to the user attitude towards the visualization of system failures.

Initial trust to the system seems to maintain the trust even if the observed system behavior clearly deviates from expected. If the users encounter an unexpected behavior for the first time, they tend to justify it in a plausible way. However, this holds only if the user interface leaves the users space to interpret the ambiguous behavior.

For example, in one scenario the user was getting a route to a selected friend (see Figure 1, left). Once the friend was located and the route was drawn, the friend's picture has suddenly disappeared from the screen (see Figure 1, right).

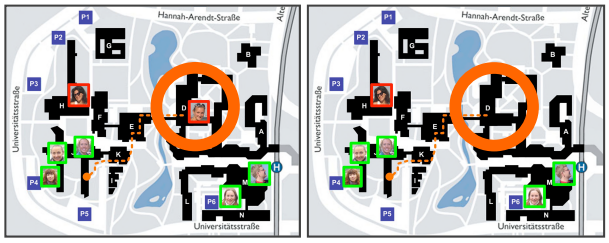

Figure 1. Example scenario of system failure.

The participants were not explained the reason of unexpected disappearing of the picture. Generally, it could have been caused by a service failure, a bug, or a UI update. However, the participants immediately tried to find a positive realistic explanation for the case. "*Probably she (the selected friend) has just logged off the system*", "*Perhaps she is changing her position at the moment, and the system just needs time to update the map*". As a result, the students rated the case not as a high trust-critical (M: 2,83; D: 0,41).

Another example simulated the immediate navigation with the mobile projector. The user was navigated on the route using the arrow view. Suddenly the arrow was pointing to an unreal direction, such as up to the ceiling or to a wall. Although the students rated this event as an obvious system error (M: 4,4; D: 0,55), they still tended to make up a realistic explanation: "*The arrow pointing up may mean: Enter the next door*".

In another scenario the user was ranking a picture on Media Wall. The user wanted to give five stars to a chosen picture; however, when submitting the result, only three stars were shown. The event was generally found trust-critical and interpreted as a failure (M: 4,33; D:0,51). However, the participants still tended to explain the situation positively: "*Probably it is an average ranking which is shown now… So, my five stars are merged with the ranking of others, resulting in three.*"

Generally, if an error happens for the first time, and the users did not experience system failures before, they are ready to "forgive" the strange system behavior. They tend to find a plausible

explanation that fits to the usage scenario. This observation can be referred to the stages of actions introduced by Norman [8]. If there is a gap between perception and interpretation stages, the users still have a freedom to make up their own interpretation and thus find a plausible explanation to the observed event.

The freedom in interpretation however may cause further "by-products". An interesting phenomenon we discovered during the study, related to users' raised expectations about the trusted system. If the initial trust is established, and users had good experiences with the system in the past, a sudden error may be explained as an additional functionality.

In one example scenario the user was getting a route to a selected friend. Suddenly the picture of the friend has moved to another place. The users not only found a plausible explanation to the unexpected behavior - "*The person has just moved from one place to another. The system updates it correctly.*" - but also they saw an additional functionality in the sudden event: "*Look! The system also works outdoors! It switches automatically between indoors and outdoors!*" Such raised expectations, however, may be dangerous for the future development of user trust. If the user realizes that the "newly discovered feature" was a system failure, the established trust can be damaged even more seriously than if the failure was detected immediately.

If the visualization of system failure be interpreted in different ways, the users clearly identify the error. In this case there is no gap between Norman's evaluation stages: the users are able to perceive, interpret and evaluate the system state in a single way. If the screen state clearly shows a wrong behavior, the users will register the failure, and as a consequence, diminish their trust.

A preview positively impacts the user trust, even in case of a system failure. Another finding from the study has shown that a preview of the expected result slightly improves the user trust, even if the final result fails. Comparing the trust rankings for picture uploading scenarios, we can see that the scenarios with preview received slightly better rankings (M: 4,8; D: 0,45) than the scenarios without a preview (M: 5; D:0). In both scenarios the finally uploaded picture was a wrong one, even though in the preview showed the correct picture. The follow-up discussion clearly revealed participants' preferences to have the visual preview.

Returning to the scenario with picture ratings on Media Wall, we have seen that the preview of the intended star-rating has softened the participants' trust evaluation. When the user selected five stars to submit, this pre-selection was displayed on the public screen. Even though the final result failed (only three stars were submitted) and the participants have clearly detected the failure, they still did not estimate the event as absolutely trust-critical (M: 4,33; D:0,51).

The positive influence of the preview on user trust can be explained as by establishment of intermediate trust: if the users are able to perceive the desired result visually, they built intermediate trust to the action. Even if the action fails at the end, the established intermediate trust contributes to the resulting trust "score".

Higher privacy tolerance to Spontaneous Spectators than to Active Interactors. When interacting alone in front of the public display, the users did not mind to open their own data and the data of their friends. According to our findings, such data as the names, pictures, and availability was found tolerable to show on a public screen. The publishing of this data was considered to be based on social network rules: if people open their data, they are aware that someone can see it.

Interestingly, the user attitude towards the private data radically changes, if a second user comes to interact with the display. Some of our scenarios simulated the situations when two users simultaneously used the public display. For example, both users render their social networks on the display. Although in a single-user scenario study participants were tolerant to the presence of possible spectators, in the scenario with an active second user the participants strongly preferred to hide all personal data. The scenario where all friends of the user remained on the screen in presence of a second user was rated as highly trust-critical (M: 4,17; D:0,41).

Therefore, the personal data related to the user or their friends should be hidden when other users actively interact with the shared display.

The observation can be mapped to the user roles described by Kaviani et al. [4] The disclosure of private information is acceptable when the user is surrounded by spectators and bystanders. Their attention to the display may be considered as implicit: they may watch the content, but rather spontaneously and unintentionally. However, once the others become the actors actively using the display, their attention to private data becomes explicit. Therefore, there is an urgent need to protect the private data.

This attitude is also in line with the rules of the social networks: "*If a friend entrusts to me his private information, it does not mean he entrusts it to the bystanders".* Indeed, most of the modern social networks (e.g. Facebook [1]) open private information only on base of an approved friendship.

As a result, in the presence of other actors, the students would strongly prefer to hide or mask the personal data of their friends. Figure 2 shows an example how the public screen can adapt to the presence of a second user: the friends of both users can be depicted by small icons. Such solution was positively rated by users, in terms of trust (M: 1,33; D: 0,52).

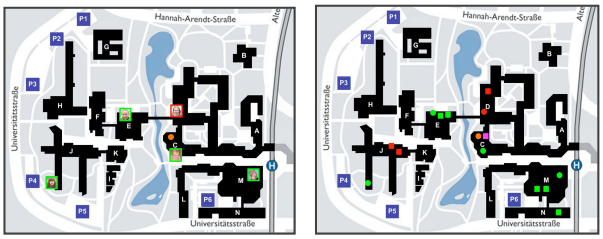

Figure 2. Adaptation of public display to the presence of the second user: masking personal data with icons

Another solution would be to move personal friends of each user to mobile displays and leave only common friends on the public display (M: 1,83; D: 0,41). However, such solution significantly reduces the benefit of the public display: basically, all interaction would now happen on the mobile screen.

5. CONCLUSION AND PERSPECTIVES

We presented a trust-centered user study aimed to find out which data and events are seen trust-critical in a multi-display scenario. The study was based on example multi-display applications that

are aimed to run on public displays located at the university and private mobile displays of the students.

The study provided interesting insights in user attitudes towards trust-critical data and events. Generally, the study participants were tolerant to open their personal data as well as the data of their social network. This holds however, only if the user interacts with the display alone, meaning that the other people are spectators or by-standers. If another user starts to interact with the same display, the observation becomes explicit, and the disclosure of private data may harm user trust. Therefore, the private data should be hidden or masked.

Along with disclosure of private data, system failures and automatic content adaptation can potentially diminish user trust. The study revealed several trends in the user attitude towards these trust-critical events. If a system failure is visualized in a way that can be interpreted in a plausible way, the users tend to find a justification to the observed system behaviour. However, if the visualization obviously deviates from the expected result, and can be interpreted in a single way, the users immediately detect the failure. A preview of the intended result seems to improve the user trust, even if the final result fails.

As a future direction, we plan to investigate more in detail the strategies how the user interface can maintain and re-establish user trust.

ACKNOWLEDGEMENTS

This research is partly sponsored by OC-Trust (FOR 1085) of the German research foundation (DFG).

6. REFERENCES

[1] Facebook www.facebook.com

[2] Glass, A., McGuiness, D., and Wolverton, M. Toward Establishing Trust in Adaptive Agents. In *Proceedings of Intl. Conference on Intelligent User Interfaces* (Gran Canaria, Spain, 13-16 January, 2008), IUI'08. ACM, New York, NY, 227-236.

[3] Graham, C., Cheverst, K. Guides, Locals, Chaperones, Buddies and Captains: Managing Trust through Interaction Paradigms. In *Proceedings of Workshop 'HCI on Mobile Guides' at MobileHCI'04* (Glasgow, Scotland, UK, September 13, 2004).

[4] Kaviani, N., Finke, M., Fels, S., Lea, R., and Wang, H. What goes where?: designing interactive large public display applications for mobile device interaction. In *Proceedings of Intl. Conference on Internet Multimedia Computing and Service* (Kunming, Yunnan, China, November 23-25, 2009), ACM, New York, NY, 129-138.

[5] Kray, C., Kortuem, G., and Krüger, A. Adaptive navigation support with public displays. In Proceedings of Intl. Conference on Intelligent user interfaces (San Diego, CA, USA, January 9-12, 2005), IUI'05. ACM, New York, NY, 326-328.

[6] Mokka, S., Väätänen, A., Heinilä, J., and Välkkynen, P. Fitness computer game with a bodily user interface. In *Proceedings of Int. Conference on Entertaining Computing* (Pittsburg, Pennsylvania, May 8-10, 2003), ICEC'03. Carnegie Mellon University Pittsburgh, PA, 1-3.

[7] Nenonen, V., Lindblad, A., Häkkinen, V., Laitinen, T., Jouhtio M., and Hämäläinen, P. Using Heart Rate to control an interactive game. In *Proceedings of SIGCHI Conference on Human Factors in Computing Systems* (San Jose, CA, USA, 28 April - 3 May, 2007), CHI'07. ACM, New York, NY, 853-856.

[8] Norman, D. The Design of Everyday Things, 1988.

[9] Polar Electro, www.polar.fi

[10] Roecker, C., Hinske, S., and Magerkurth, C. Intelligent Privacy Support for Large Public Displays. In *Proceedings of the Conference on Universal Access in Human-computer Interaction* (Beijing, China, July 22-27, 2007), Springer-Verlag, Berlin Heidelberg, 198-207.

[11] Rukzio, E., Schmidt, A., and Krüger, A. The rotating compass: a novel interaction technique for mobile navigation. In *Proceedings of SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA, April 4-9, 2009), CHI'09. ACM, New York, NY, 113-122.

[12] Shneiderman, B., and Maes, P. Direct Manipulation vs. Interface Agents, *Interactions* 4(3) (November/December 1997), 42-61.

[13] Villar, N., Schmidt, A., Kortuem, G., and Gellersen, H. Interacting with Proactive Community Displays, *Computers & Graphics Magazine* 27 (2003), 849-857.

[14] Vogel, D., and Balakrishnan, R. Interactive Public Ambient Displays: Transitioning from Implicit to Explicit, Public to Personal, Interaction with Multiple Users. In *Proceedings of the ACM symposium on User interface software and technology* (Santa Fe, NM, USA, October 24–27, 2004), UIST'04. ACM, New York, NY, 137-146.