Friend or Foe? Relationship-Based Adaptation on Public Displays

Ekaterina Kurdyukova, Karin Bee, and Elisabeth André

University of Augsburg, Universitaetsstrasse 6a,
86159 Augsburg, Germany
{kurdyukova,karin.bee,andre}@hcm-lab.de

Abstract. Personalization of content on public displays is likely to cause the disclosure of user's private data. In order to protect the user's privacy, different protection strategies are used, e.g. the private data is hidden, occluded or blurred. Existing systems usually follow a uniform protection strategy, applying it every time a spectator is detected in the display proximity. However, the necessity in privacy protection often depends on the personal relationships between the user and the spectator. This work investigates how the relationship context influences user preferences in adaptation strategies. Additionally, we study how privacy level of data and the presence of a mobile device influence this preference. The obtained results can guide adaptation designers in creation of more flexible privacy protection mechanisms.

1 Introduction

Modern public displays utilize various strategies to protect private data, e.g. occluding, removing, or blurring the private content. As a rule, these techniques are uniformly applied every time a spectator is detected near the display [1, 2]. However, user willingness to expose or hide private content usually depends on the relationship with the spectator. Thus, people may want to demonstrate the content to their close friends, but protect it from the eyes of a stranger.

Different protection strategies can be applied to different relationships. Similarly to the trusted groups in social networks (such as Facebook), spectators can be classified into groups. Each group is assigned a specific adaptation strategy, providing stronger or weaker data protection.

This paper aims to investigate how relationship context impacts user preferences in adaptation strategies. Using two example applications, designed for community public displays, we analyze user attitudes towards protection necessity in different scenarios. Besides the relationship context, we take a look at additional context sources such as privacy level of content and the presence of a mobile device in the setting.

After an overview of the existing privacy protection techniques, we motivate the need for relationship-based adaptation. Then, we describe the experiment, comment on the obtained results, and discuss their application in adaptive public displays.

2 Privacy Protection on Public Displays

Adaptation aimed at the personalization of content is widely utilized on public displays. For example, it facilitates the selection of relevant news [3], gives the audience more details about the speaker [4], or reminds the user on important information [1, 2, 5].

Besides evident benefits, the personalization brings the risk of privacy disclosure [4]. In order to avoid the disclosure, public displays can adapt to the presence of spectators using various protection strategies. The protection power of these strategies may vary from strong, such as a complete removal of private data from the display, to very low, e.g. doing nothing or just minimizing the size of the private content. All in all, the display reaction aimed at privacy protection can be classified into the following groups, ordered by ascending protection power:

1. ***Do Nothing***: the display is insensitive to the presence of spectators. All private data remains on the screen [4].

2. ***Minimize***: private content is minimized in size, or changes its transparency [2] or sharpness. Spectators can still view the private data, though the visual access to the data is hampered. The user can continue interaction with the data.

3. ***Mask***: private content on the display is occluded with blinders [6], pixelized [7], or covered with some neutral display elements [6]. Spectators can clearly see that some content is hidden; however, they cannot view the content itself. Since the private data is protected, users need to interrupt the interaction.

4. ***Remove Private Part***: if the personalized content is partially neutral (e.g. selected news) and partially private (e.g. user's name), protection mechanism removes only the private part from the display. Spectators cannot notice that some content is hidden or missing [8]. Users have to interrupt the interaction.

5. ***Remove All***: All personalized content is removed from the public screen. Spectators cannot notice that the content is hidden; user interrupts the interaction.

Existing adaptive displays usually follow a uniform protection strategy independently on the personality of the spectator. Such a uniform privacy protection brings certain inflexibility into the system, since the concept of privacy depends on the relationship with the spectator [9, 10]. People's need to differentiate between trusted groups can be clearly seen on the example of social networks [11]. In online network communities, users specify unique policies for the groups of friends, family, colleagues, etc. and thus control the access to their private data [12]. The need in such relationship-based trusted groups also holds for public displays. The system should be able to determine the group of the current spectators and perform the adaptation according to the group's policy. Such relationship-based adaptation will not only increase the comfort of interaction, but also will increase user trust [13].

Although modern researchers often emphasize the need for a flexible relationship-based adaptation [9, 10, 11], there is no research in the domain of public displays that studies this question in greater details.

Besides the relationship context, other factors influence the necessity in data protection: for example, privacy level of content [1] and the current technical setting [14]. Modern research proposes diverse technical settings for interaction with public displays, starting from mobile devices [14], tablet-PCs, and finishing with AR-helms and stereoscopic glasses [7]. Since our work focuses on the settings available and familiar to a wide range of users, we consider two typical settings: only a public display (*PD-only*) and a public display assisted by a mobile device (*PD-mobile*). Other contexts, such as user activity, current task, etc. might also influence the protection necessity. However, they are often task-dependent and thus their impact is hard to generalize.

3 Studying the Relationship-Based Adaptation

To summarize, this paper aims to tackle the following questions:

- How does the relationship with the spectator influence user choice of protection strategy on public displays?
- How does privacy level of content influence this choice?
- How does presence of a mobile device in the setting influence this choice?

3.1 Prototypes

In order to address these questions, we arranged an experiment with two public display applications. The applications, called Friend Finder and Media Wall represent typical content for community public displays: support of a social network and a media gallery. Examples of these content types can be frequently encountered in research works [15, 16, 17, 18, 19], as well as in real-life projects, such as Interactive Video Wall in Copenhagen [20] or CityWall in Helsinki [19]. The examples show that despite the awareness of privacy issues [17, 21] caused by the personalized content, people do place their private data on public displays and do need to protect it. Below we describe our applications more in details.

Friend Finder visualizes a user's social network overlaid over a local map (see Fig.1). The users can browse through their peers and retrieve the directions to them. The public display can be operated via a mobile phone client or by means of gestures. An earlier conducted study [22] revealed that the peers' names, pictures, and locations are considered as privacy-critical data. Therefore, a privacy protection mechanism was integrated into Friend Finder: the display executed a uniform masking of peers' pictures and names once a spectator was detected in the proximity [23]. However, intermediate evaluations uncovered the need for a more flexible adaptation: users were willing to protect their data only from certain individuals.

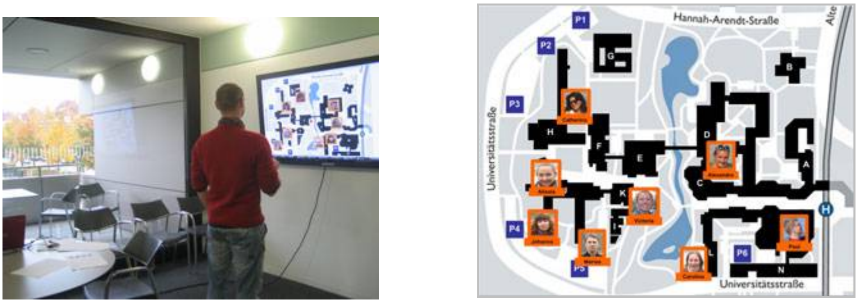

Fig. 1. Friend Finder visualizes user's social network on a public display

Media Wall presents a collection of media shared by community members. Users can upload and edit their media in the working space (see Fig. 2), view and rank the media of the others. Since privacy concerns are likely to arise when uploading the private media [17, 22], an adaptive protection was required. The need in protection depended on the privacy level of media content and on the spectator personality.

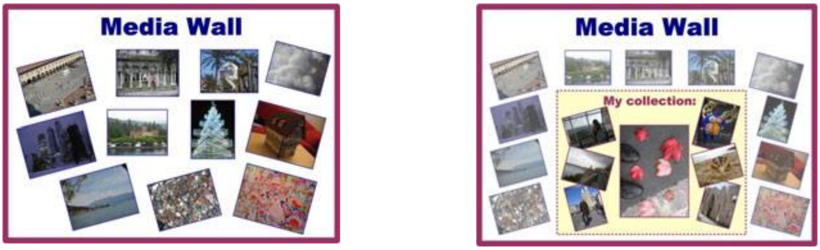

Fig. 2. Media Wall: start screen (left) and personalized working space (right)

For the experiment we created several prototypes of each system which differed by the privacy levels and by settings. For Friend Finder, two levels of privacy were provided. The higher privacy version (Friend Finder 2) showed peers' names and portrait pictures (see Fig. 1, right). The lower privacy version (Friend Finder 1) showed only names and uniform icons instead of the pictures. For Media Wall, three levels of privacy were created. The low privacy version (Media Wall 1) showed the personalized collection of neutral pictures, e.g. nature or sightseeing views containing no people or the user alone. The medium privacy version (Media Wall 2) showed the pictures containing the user and friends, but with no confusing content. Finally, the high privacy version (Media Wall 3) exposed the pictures with some compromising content: the user and friends in late party scenes, beach bikini scenes, etc.[1]

Each prototype provided five adaptive strategies aimed at privacy protection. Here, as private data we denote: peers' names for Friend Finder 1, peers' names and pictures for Friend Finder 2, personal collection for Media Wall. The adaptive strategies were executing the following actions:

1. Do Noting: private data remained on the display.

2. Minimize: private data was shrunk in size, but remained on the display.

3. Mask: private data was occluded with solid blinders.

4. Remove Private Part: private data was completely removed from the screen. The neutral elements, such as uniform icons (Friend Finder) and working space (Media Wall) remained on the public screen.

5. Remove All: all private data was removed; the screen showed only the map.

The prototypes were presented in *PD-only* and in *PD-mobile* settings. The *PD-mobile* setting supported the strategies ***3-5*** where private data was not visible on the public screen: the private data migrated to the mobile screen, enabling the users to continue interaction.

[1] Our estimation of privacy levels was verified during the experiment; it matched the estimation of the participants.

All in all, ten prototypes were presented to each test participant: Friend Finder 1 and 2, in *PD-only* and *PD-mobile* setting, and Media Wall 1,2, and 3, also in *PD-only* and *PD-mobile* setting.

3.2 Experiment Procedure

Seventeen persons participated in the experiment, 7 female and 10 male, aged from 23 to 37 (average 29,3). Among them there were Italians, Russians, Ukrainians, Chinese, Germans, and a Bosnian, working in banking, marketing, Engineering, Economics and Multimedia research, or studying at the University. All of them have experiences with social networks, such as Facebook, Studi-vz, XING, LinkedIn, myspace, InterNations; 12 persons have online photo collections.

At the beginning of the experiment we introduced shortly the topic of adaptation on public displays, demonstrated possible adaptation strategies, and presented our two applications, Friend Finder and Media Wall.

Then every participant was asked to imagine three individuals: a close friend, an acquaintance, and a stranger. The friend and the acquaintance should have been real persons (we asked to name them): the friend – a close trusted person and the acquaintance – a neutral familiar person, e.g. a colleague or a neighbor. The stranger was described by a uniform portrait: a male unfamiliar person, in his forties.

In the main part of the experiment the participants were asked to evaluate the adaptation strategies for the prototypes, first Friend Finder and then Media Wall. Every prototype was shown first in *PD-only* setting, and then in *PD-mobile*. The order of privacy levels within prototypes was counterbalanced. For every prototype we first demonstrated all five adaptation strategies. Then we asked the participants to imagine the following scenario. The participant interacts with the public display alone and uploads the private data. Then a spectator suddenly approaches the display. We asked which of the presented adaptation strategies would be preferred if the spectator was the friend, the acquaintance (named), or the stranger.

4 Results

The preferences of the participants were noted down as numbers from 1 to 5, referring to the strength of protection strategies (1 = ***Do Nothing***, 5 = ***Remove All***). The results were analyzed statistically, by comparing the preferences in various prototypes with pared t-test. Below we report on the results and give our comments.

4.1 Relationships Matter

As we assumed, participants consistently chose stronger protection strategies for less close relationships. Significant differences were obtained through all the results for Friend Finder and Media Wall, in *PD-only* and *PD-mobile* settings (see Fig. 3).

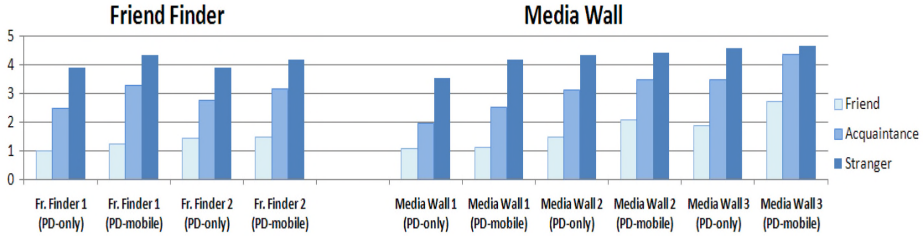

Fig. 3. Preferences in protection strategies for different relationships with spectators

Only for the stranger observing Media Wall 2 or Media Wall 3 in *PD-mobile* setting, the participants chose the strongest protection for both privacy levels.

4.2 Relationship Context in Friend Finder

Figure 4 summarizes the preferences in protection strategies for Friend Finder. The mean values are indicated above the graph bars.

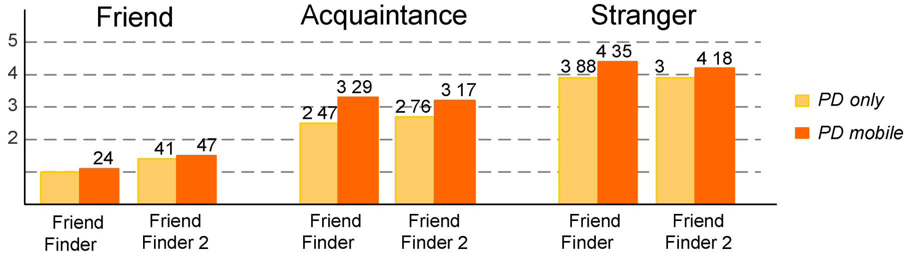

Fig. 4. Preferred protection strategies for Friend Finder in *PD-only* and *PD-mobile* settings

Spectator = Friend

Different privacy levels. The higher the privacy level of the content, the stronger protection strategy is chosen. Thus, the protection strategies for Friend Finder 2 were significantly higher than for Friend Finder 1 (p = 0.024). Friend Finder 2 discloses definitely more data on the social network: while just a name (Friend Finder 1) can stand for several persons, a picture and a name (Friend Finder 2) disambiguously points at a certain person. Often a spectator-friend shares some contacts of the user. The user might not be aware of private situation between the friends. Therefore, the user might prefer to hide the connections, in order not to confuse the common friends or the spectator: "Perhaps I have his [spectator's] ex-girlfriend in my network, and I have no idea what's their relationship now".

PD-only vs. PD-mobile Setting. The presence of a mobile device does not influence the choice of the protection strategy. If the users concern about the disclosure of their contacts, they choose a stronger protection in both settings.

Spectator = Acquaintance

Different privacy levels. No significant differences were found for privacy levels: similar strategies were chosen for Friend Finder 1 and Friend Finder 2.

PD-only vs. PD-mobile Setting. In *PD-mobile* setting the participants chose stronger protection than in *PD-only* setting. Friend Finder 1 (p = 0.0056) and Friend Finder 2 (p = 0.034). In the *PD-only* setting the users often sacrifice their privacy concerns for the sake of interaction comfort. Even under observation of an acquaintance, users choose less protective strategies which still enable them to proceed with interaction. The presence of a mobile device, however, eliminates the need to sacrifice the privacy; the mobile device enables further interaction and secures the private data. Therefore, a stronger protection is chosen on public display.

Spectator = Stranger

No significant differences were found for the stranger case. For both settings, *PD-only* and *PD-mobile*, independently on the privacy level, the preferences were spread between the stronger strategies ***3-5,*** which ensure invisibility of the private data.

4.3 Relationship Context in Media Wall

Figure 5 summarizes the preferences in protection strategies for Media Wall, showing the mean values above the graph bars.

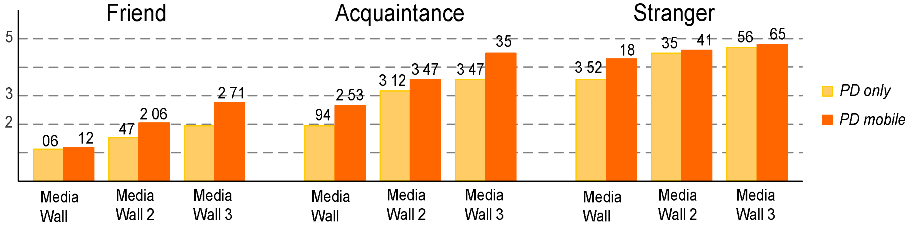

Fig. 5. Preferred protection strategies for Media Wall in *PD-only* and *PD-mobile* settings

Spectator = Friend

Different privacy levels. If a friend is observing the display, a strong protection is necessary only for highly private data. Thus preferences for Media Wall 3 were significantly higher than for Media Wall 1 (p = 0.0072) and for Media Wall 2 (p = 0.045). Highly private media often contain private information not only about the user, but also about their friends. Therefore, users prefer to hide the media in order not to confuse their friends who are even not aware of the possible disclosure.

PD-only vs. PD-mobile Setting. The protection preferences were significantly lower in *PD-only* setting than in *PD-mobile* setting, for medium (p = 0,038) and high (p = 0,015) privacy level. This result can be again explained by users' readiness to sacrifice their privacy concerns for the sake of interaction comfort: in *PD-only* setting users choose a weaker protection which does not impair the interaction. If a mobile device is available, the users continue the interaction on the mobile device and set a stronger protection on public display.

Spectator = Acquaintance

Different privacy levels. The higher the privacy level, the significantly stronger strategies were chosen, throughout all privacy levels.

PD-only vs. PD-mobile Setting. Low and high privacy levels require significantly stronger protection in *PD-mobile* setting than in *PD-only:* Media Wall 1 (p = 0,01) and Media Wall 3 (p=0,021). The protection for medium privacy level strongly depends on the role of the acquaintance. Users tend to decide once, if it is acceptable to show the content to the acquaintance and hold the decision for any setting.

Spectator = Stranger

Different privacy levels of content matter in *PD-only* setting. Medium and highly private data need significantly stronger protection than the low privacy level.

PD-only vs. PD-mobile Setting. The mobile device influences user decision only for low level privacy data: a stronger protection is chosen in PD-mobile (p = 0,043). For other privacy levels, the highest possible protection is chosen in either setting.

Discussion: Applying the Results

The results obtained in the experiment can be summarized as follows:

- **For a Friend-Spectator**, generally no protection is needed. The privacy concerns arise only if the display content can confuse the spectator-friend or compromise the persons involved in the content. In *PD-only* setting the users still keep the data opened, since hiding or removal is likely to impair the interaction process. In *PD-mobile* setting users tend to choose a higher protection: the mobile display serves as a safe depot for private data and enables further interaction with the content.

- **For an Acquaintance-Spectator**, a stronger protection is required. However, the preferences can be widely spread. Such distribution is caused by diverse roles of acquaintances. For instance, users may expose their holiday pictures to a neighbour, but prefer to hide them from a colleague. Having a mobile device available, the users tend to choose a stronger protection.

- **For a Stranger-Spectator**, the strongest protection is preferred. Since the users are not aware of intentions or interests of the stranger, they prefer to protect even the low privacy data. The presence of a mobile device barely influences the protection preference: the users choose the strongest protection in either setting.

The obtained results can inform the design of a real-time relationship-based adaptation. The relationship information can be retrieved from the structure of user's social network (such as Facebook), from the intensity of chat and phone conversations. The personality of the spectator can be identified in real time by camera-based face recognition or by means of mobile phone ID. Additional context analyzed in our experiment can be also retrieved automatically. The setting context can be derived from availability of a mobile device. The privacy level can be extracted from the display content. For instance, if several faces are detected on a picture, the picture is automatically set to medium or high privacy.

Privacy concerns vary greatly among the users; they depend on the personality, traits of the character, personal experiences and can be summarized as *trust* *disposition* [13]. In our experiment, we noticed that independently on nationality, gender, or age, participants showed some trust patterns, e.g. some of them concerned more about privacy in social networks, others – about private pictures. Therefore, the definition of “universally applicable” privacy levels still remains a challenging task.

The preferences found in the experiment can serve as recommendations for adaptation design for the diverse contextual settings. However, designers should always provide the users with leverages to override the automatic adaptation, so that the users feel the ultimate control over the system behaviour.

Conclusion

Relationship context can make the adaptation on public displays more flexible. By means of the literature review and the conducted experiment, we showed that personal relationships with spectator significantly impact the user’s preference in adaptation strategy. Using example applications, we analyzed how this preference is influenced by privacy level of content and by the presence of an assisting mobile device. The reported results can guide the designers in creation of intelligent relationship-based adaptation mechanisms.

References

1. Cao, H., Olivier, P., Jackson, D.: Enhancing privacy in public spaces through crossmodal displays. Journal Social Science Computer Review 26(1), 87–102 (2008)
2. Vogel, D., Balakrishnan, R.: Interactive Public Ambient Displays: Transitioning from Implicit to Explicit, Public to Personal, Interaction with Multiple Users. In: UIST 2004 (2004)
3. Villar, N., Schmidt, A., Kortuem, G., Gellersen, H.: Interacting with proactive public displays. Computers and Graphics 27(6), 849–857 (2003)
4. McCarthy, J., McDonald, D., Soroczak, S., Nguyen, D., Rashid, A.: Augmenting the Social Space of an Academic Conference. In: Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW 2004, pp. 39–48. ACM Press, New York (2004)
5. Rukzio, E., Mueller, M., Hardy, R.: Design, Implementation and Evaluation of a Novel Public Display for Pedestrian Navigation: The Rotating Compass. In: Proceedings of the Conf. on Human Factors in Computing Systems, CHI 2009. ACM Press, New York (2009)
6. Röcker, C., Hinske, S., Magerkurth, C.: Intelligent Privacy Support for Large Public Displays. In: Stephanidis, C. (ed.) UAHCI 2007 (Part II). LNCS, vol. 4555, pp. 198–207. Springer, Heidelberg (2007)
7. Boyle, M., Edwards, C., Greenberg, S.: The Effects of Filtered Video on Awareness and Privacy. In: Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW 2000, pp. 1–10. ACM Press, New York (2000)
8. Shoemaker, G.: Supporting Private Information on Public Displays. In: Extended Abstracts on Human Factors in Computing Systems, CHI 2000, pp. 349–350. ACM Press, New York (2000)

9. Fraser, K., Rodden, T., O'Malley, C.: Trust, Privacy and Relationships in 'Pervasive Education': Families' Views on Homework and Technologies. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 180–197. Springer, Heidelberg (2007)
10. Iachello, G., Smith, I., Consolvo, S., Chen, M., Abowd, G.: Developing Privacy Guidelines for Social Location Disclosure Applications and Services. In: Proceedings of the Symposium on Usable Privacy and Security, SOUPS 2005, pp. 65–76. ACM Press, New York (2005)
11. Palen, L., Dourish, P.: Unpacking "Privacy" for Networked World. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2003, pp. 129–136. ACM Press, New York (2003)
12. Jones, S., O'Neill, E.: Feasibility of Structural network clustering for group-based privacy control in social networks. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS 2010. ACM Press, New York (2010)
13. Lumsden, J., MacKay, L.: How does personality affect trust in B2B e-commerce? In: Proceedings of the International Conference on Electronic Commerce, ICEC 2006, pp. 471–481. ACM Press, New York (2006)
14. Rukzio, E., Schmidt, A., Hussmann, H.: An Analysis of the Usage of Mobile Phones for Personalized Interactions with Ubiquitous Public Displays. In: Proceedings of the Workshop on Ubiquitous Display Environments (2004)
15. Congleton, B., Ackerman, M., Newman, M.: The ProD Framework for Proactive Displays. In: Proceedings of the ACM Symposium on User Interface Software and Technology, UIST 2008, pp. 221–231. ACM Press, New York (2008)
16. Huang, E., Mynatt, E.: Semi-Public Displays for Small, Co-located Groups. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2003, pp. 49–56. ACM Press, New York (2003)
17. Holleis, P., Rukzio, E., Otto, F., Schmidt, A.: Privacy and Curiosity in Mobile Interactions with Public Displays. In: Adjunct Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2007 (2007)
18. Greaves, A., Rukzio, E.: View & Share: Co-Present Viewing and Sharing of Pictures using Personal Projectors. International Journal of Mobile Human Computer Interaction (2010)
19. Peltonen, P., Salovaara, A., Jacucci, G., Ilmonen, T., Ardito, C., Saarikko, P., Batra, V.: Extending large-scale event participation with user-created mobile media on a public display. In: Proceedings of International Conference on Mobile and Ubiquitous Multimedia, MUM 2007, pp. 131–138. ACM Press, New York (2007)
20. http://museummedia.nl/2011/04/museum-of-copenhagen-interactive-video-wall-housed-in-a-shipping-container/
21. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, pp. 237–245. Springer, Heidelberg (2002)
22. Kurdyukova, E. André, E., Leichtenstern, K.: Trust-centered Design for Multi-Display Applications. In: Proceedings of international conference on Advances in Mobile Computing & Multimedia, MoMM'10, pp. 415 – 420. ACM Press, New York (2010).
23. Kurdyukova, E.: Designing Trustworthy Adaptation on Public Displays. In: Konstan, J.A., Conejo, R., Marzo, J.L., Oliver, N. (eds.) UMAP 2011. LNCS, vol. 6787, pp. 442–445. Springer, Heidelberg (2011)