Röcker, C., Hinske, S., Magerkurth, C. (2009). Information Security at Large Public Displays. In: M. Gupta, R. Sharman (Eds.): *Social and Human Elements of Information Security: Emerging Trends and Countermeasures.* IGI Publishing, Niagara Falls, NY, USA, pp. 471 - 492.

Information Security at Large Public Displays

Carsten Röcker[(1)], Carsten Magerkurth[(2)] and Steve Hinske[(3)]

[1] Department of Cognitive Science, University of California, San Diego
9500 Gilman Drive, La Jolla, CA 92093-0515, carsten@hci.ucsd.edu

[2] SAP Research, CEC St. Gallen
Blumenbergplatz 9, CH-9000 St. Gallen, Switzerland, carsten.magerkurth@sap.com

[3] Institute for Pervasive Computing, ETH Zürich
Clausiusstr. 59, 8092 Zürich, Switzerland, steve.hinske@inf.ethz.ch

Abstract. In this chapter we present a novel concept for personalized privacy support on large public displays. In a first step, two formative evaluations are conducted in order to analyze the requirements of potential users regarding the protection of private information on large public displays. The insights gained in these evaluations are used to design a system that automatically adapts the information visible on public displays according to the current social situation and the individual privacy preferences of the user working on the display. In a third evaluation, the developed system is evaluated regarding its appropriateness for daily usage and its usefulness to protect privacy. The results of the evaluation show that users are in general willing to trust system-based protection mechanisms, provided that they are well implemented. In this context, the proposed combination of pre-defined privacy profiles and context-adapted information visualization proved to be a good trade-off between usability and adequate privacy protection.

1 Introduction and Motivation

A continuous trend towards higher mobility is observable in most companies, with employees spending considerable time away from their own desk, working in meeting rooms, other offices or in the hallway (Lamming et al., 2000). According to estimates, white-collar workers spend between 25% and 70% of their daily working time in conferences or meetings with colleagues (Eldridge et al., 1994; Whittaker et al., 1994). As large-screen displays are becoming increasingly prevalent in public spaces (Churchill et al., 2004), several projects address this evolution by providing 'walk-up-and-use' applications on large screens in public or semi-public areas. *Blue Board* (Russell & Gossweiler, 2001), for example, is a large plasma display with touch sensing and a badge reader to identify individuals. The onboard software is designed for personal use as well as small group collaborative usage. While *Blue Board* requires users to set up their content ahead of time and thus gives the user control over the information that is displayed, other systems, like *IM Here* (Huang et al., 2004), are designed for more spontaneous workgroup interaction. *IM Here* is a shared instant messaging system running on a large public display designed to facilitate informal communication while away from the desktop. Similar to (Huang & Mynatt, 2003), upcoming privacy and security problems are eluded by restricting the usage of the systems to small groups of users.

Although privacy guidelines have been available for quite some time (e.g., Langheinrich, 2001; Bellotti & Edwards, 2001) most developers still rely on social protocols or do not address privacy questions at all when designing applications for large public displays. Until today, there are very few approaches that help users with preserving their privacy while working on large displays in public places. In most cases (e.g., Rekimoto, 1998; Greenberg et al., 1999), additional private displays are used to generate and present personal information, while public information is displayed on a shared large display. A different approach using a stereographic display and special

shutter glasses is described in (Shoemaker & Inkpen, 2001). Personal privacy is maintained through the filtering of the information on the shared display. Users wearing shutter glasses see the information publicly available as well as their own private information, while other people's private data is not visible to them. A similar system was developed by Yerazunis & Carbone (2002), which uses time-masked images to ensure privacy. As the system requires CRT displays with higher-than-usual screen refresh rates and special eyewear, the usage of the system is likewise restricted. Comparable systems were developed by Eaddy et al. (2004), Needham & Koizumi (1998) and Berger et al. (2005).

Although all approaches support individual privacy in an adequate way, they always require additional personal devices like PDAs or shutter glasses. But as most public displays are intended for walk-up-and-use applications, existing solutions are not very suitable.

The goal of the research work presented in this chapter is to give users the freedom to spontaneously work on large public and semi-public displays without being afraid of possible privacy infringements through passers-by. In contrast to existing approaches, we aimed at providing users with a system that automatically controls the information that is visible to others, but without requiring users to employ any additional equipment.

2 Formative Evaluation of User Requirements

In order to provide trusted mechanisms for privacy protection, it is most crucial to involve potential users in the design process right away from the beginning. Therefore, the requirements of potential users regarding privacy and security issues in multi-user situations were analyzed in two questionnaire-based evaluations.

The emphasis of the first evaluation was on data-related questions, especially on the willingness to disclose different types of information in the work environment and on the acceptance of system-controlled privacy measures. In the second evaluation we intended to analyze the system and interface requirements of potential users regarding the protection of private information on large public displays.

2.1 Analysis of Information Requirements

In order to guarantee satisfactory privacy protection while simultaneously minimizing interruptions during the work process, it is essential to know which information should be hidden from whom and when. Protecting work-related information from colleagues passing-by might not be necessary and doing so would most likely result in an unintended interruption of the ongoing task; but the situation is fundamentally different, when other people approach the display while the user is accessing private information.

In a first step, a questionnaire-based survey was carried out to investigate potential privacy concerns. The topic was addressed by investigating the demands of potential users regarding workplace-related information. This was done to obtain a deeper insight in the requirements for privacy in multi-user situations and establish a basis for the development of an appropriate concept. The emphasis of the survey was on privacy-related questions, especially on the importance of privacy in office environments, and the willingness to share personal information with co-workers. In order to get representative results, a target group outside the research community was chosen. This is of particular importance, as the majority of office workers will lack a detailed technical knowledge. The survey was conducted during an open house day at the Fraunhofer Institute for Integrated Information and Publications Systems (IPSI) in Darmstadt, Germany. The age distribution is shown in Table 1.

Table 1: *Age distribution (N=131).*

Age	**15 -20**	**21-25**	**26-30**	**31-35**	**36-40**	**41-45**	**46-50**	**51-55**	**56-60**
Frequency	8	43	37	17	8	4	5	6	3
Percentage [%]	6.1	32.8	28.2	13.0	6.1	3.1	3.8	4.6	2.3

Being asked about their computing skills, 51.1 % rated themselves as advanced, 42.2 % as experts und 6.9 % as beginners (see Table 2). The survey shows that 45.0% of all users rate privacy 'important' and 32.8% as 'very important', while at the same time over one third (36.6%) never change their passwords. The results stress again the important role of privacy in ubiquitous computing environments (Lahlou et al., 2005), but also indicate a large discrepancy between the users' desire to protect privacy and their willingness to take relevant measures.

Table 2: *Importance of privacy (left) and computer skills (right).*

Importance of Privacy	**Freq.**	**Perc. [%]**
1 (unimportant)	0	0
2	9	6.9
3	20	15.3
4	59	45.0
5 (very important)	43	32.8

Computer Skills	**Freq.**	**Perc. [%]**
Beginner	9	6.9
Advanced	67	51.1
Expert	55	42.2

In the second part of the questionnaire, the participants were confronted with different types of information and asked, which information they would be willing to provide to whom.
In a local work environment, different types of information are available to those present. Depending on the degree of confidentiality, the information can be clustered into different groups. For example, some data are continuously available and immediately perceptible by everyone in the local environment (e.g., location), while other information might only be available to a certain group of people (e.g., business appointments). Besides this, there is also personal information, which is usually not meant to be shared with others, for example, the history of recently accessed web pages. To make the questions more concrete, examples of workplace information are used that represent certain categories of data. The participants had to fill out a table, containing different examples of information that could be captured in the work context and corresponding people who might have access to the information. In all questions, the captured information is used as the independent variable, and the persons, who can access the information, as the dependent variable. The following diagrams show the answers for the different types of data (percentage of possible responses, multiple responses were feasible)
Table 3 lists different types of information that is continuously available to co-workers in a local office environment. Examples for such information are the current activity, the location of a colleague, or the progress of a task a team member is currently working on.

Table 3: *Frequency and percentage of participants, who would provide different types of continuously available information to different recipients (N=131).*

	Current Activity		Current Location		Task Progress	
Information Receiver	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**
Nobody	20	15.27	25	19.08	14	10.69
Authorized Persons	40	30.53	37	28.24	45	34.35
Friends and Family	36	27.48	42	32.06	43	32.82
Colleagues	58	44.27	51	38.93	47	35.88
Superior	53	40.46	36	27.48	70	53.44
All	10	7.63	11	8.40	12	9.16

But not all workplace information is continuously perceptible to all persons in the local work environment. Some information is only available to a certain group of people, like members of a team. That information is usually not directly perceptible, but based on shared knowledge or accessible through a shared source of information like a group calendar or project plan. Examples of such information used in the questionnaire are assigned tasks and activities, business appointments, and information about previous tasks and projects.

Table 4: *Frequency and percentage of participants, who would provide different types of team internal information to different recipients (N=131).*

	Assigned Tasks		Business Appointments		Previous Tasks	
Information Receiver	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**
Nobody	9	6.87	12	9.16	10	7.63
Authorized Persons	58	44.27	53	40.46	47	35.88
Friends and Family	29	22.14	47	35.88	37	28.24
Colleagues	66	50.38	88	67.18	46	35.11
Superior	84	64.12	90	68.70	71	54.20
All	12	9.16	7	5.34	18	13.74

The third group comprises information that is personal and therefore usually not available to team members. Such information includes private appointments, hobbies and personal preferences, and data about accessed websites.

Table 5: *Frequency and percentage of participants, who would provide different types of personal information to different recipients (N=131).*

	Private Appointments		Personal Preferences		Accessed Websites	
Information Receiver	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**	**Freq.**	**Per. [%]**
Nobody	37	28.24	15	11.45	55	41.98
Authorized Persons	30	22.90	27	20.61	27	20.61
Friends and Family	71	54.20	81	61.83	21	16.03
Colleagues	7	5.34	32	24.43	13	9.92
Superior	2	1.53	10	7.63	14	10.69
All	2	1.53	17	12.98	5	3.82

The results indicate that the willingness to provide information varies widely depending on both, the type of information and the information receiver. In most cases there are differences between colleagues, superiors, and specially authorized persons. Users are generally very careful to grant others access to previously captured workplace information. Even information that is continuously visible to co-workers, like information about the current activity and task (7.63%) or location (8.40%), is not voluntarily shared with all others. The willingness to provide data is even lower for information that is usually not available to team members, for example, information about recently accessed websites (3.82%).

The third part of the evaluation investigated the acceptance of automated protection mechanisms in group situations as well as the desired degree of system support regarding privacy protection. The goal was to understand if and how users want to be supported in protecting their privacy in dynamically changing group situations. The evaluation showed that most users (83%) would appreciate a system-based mechanism helping them to protect their information privacy. While automated privacy support seems to be favored by the majority of users, most users are very reluctant to provide the necessary information to auto-configure their privacy settings. For example, less than 10% of the users would accept the collection of biometric information, even if this would significantly reduce the required manual input. The results showed that system developers must not rely on active user participation when implementing measures to safeguard user privacy, but should aim at designing easy and intuitive ways to handle personal privacy and data security in everyday situations.

2.2 User Interface Requirements

The goal of the second evaluation was to investigate how automated protection mechanisms would influence the usage of large displays in public areas. During the evaluation, different scenarios were presented to the participants in a three-step process. First and prior to the presentation of the main scenarios, the participants were asked to assess the suitability of large displays in public areas. Therefore, examples of different applications and information types were presented to the participants, which had to be rated on a five-point scale.

In the second part of the evaluation, the participants were asked to visualize a scenario where they are working on a large public display located in a hallway of an office building. Since the display (or, more explicitly, the computer it is connected to) is integrated in the company network, the display can be used as a desktop replacement (i.e., all standard application are running on it). The scenario describes a situation, where several application windows (for example, an internet browser, a document viewer, and an e-mail program) are displayed on the public display. At the end of the scenario, the participants were explicitly reminded that passers-by are likely to see what they are doing, but also that these passers-by are mostly colleagues (i.e., people they are familiar with). In the following questions, they were asked to assess their perceived privacy while working

on the display, to specify applications they would use in such a situation, and to rate the suitability of large public displays for accessing public as well as private information.
Besides this general information, we aimed at gaining specific feedback on how automated privacy protection would influence the usage of large displays in public environments. Therefore, the initial scenario was extended with a fictitious system, which automatically protects the privacy of users working on the display. The described system protects individual user privacy by automatically hiding sensitive information when other people approach the display. The participants, however, were asked not to care *how* this is achieved, but focus on the fact that they can work on the display without being afraid of potential privacy infringements.
The questions presented in the previous part were adapted to the extended scenario and had to be answered under the light of a generic privacy protection system that unobtrusively works in the background. In addition to that, the participants were asked to assess the usefulness of the presented approach and to answer several questions concerning the interface requirements of automated privacy protection systems. Altogether, N=55 people participated in the evaluation. The gender and age distribution are shown in Table 7.

Table 6: *Gender and age distribution of the participants.*

Gender Distribution			**Age Distribution**					
Male	**Female**	**Total**	**<25**	**25-34**	**35-44**	**45-54**	**>54**	**Total**
36	19	55	16	22	4	9	4	55
65.45%	34.55%	100.00%	29.09%	40.00%	7.27%	16.36%	7.27%	100.00%

In addition to the standard demographical information, the participants were asked to assess their technical experience (see Table 8).

Table 8: *Technical experience of the participants.*

Very Experienced	**Experienced**	**Average**	**Not Very Experienced**	**No Experience**	**Total**
13	16	17	7	2	55
23.64%	29.09%	30.91%	12.73%	3.64%	100.00%

It is worth noticing that in most cases there were no or only slight differences between the demographical groups.
Above all, we wanted the participants to provide us with information about how suitable they consider large displays in public areas in general (see Table 9). We listed six applications for large public displays that had to be rated on a scale ranging from 1 (very suitable) to 5 (totally unsuitable).
Over 80% of the participants considered large displays to be suitable or very suitable for displaying rather public or general content such as advertisements or traffic information. In the case of entertainment-related content or presentations, the majority (over 60%) still classified large public displays as suitable or very suitable. The remaining two applications, namely desktop replacement and internet browsing, however, turned out to be rather unsuitable for being displayed on large public displays: more than half the interviewees considered them to be unsuitable or even absolutely unsuitable.

Table 9: *Results to the answers "How suitable do you consider large displays for the following application: app" with app ∈ {advertising, traffic information, entertainment, presentations, desktop replacement, internet browsing}. The applications had to be rated on a scale from 1 (very suitable) to 5 (absolutely unsuitable).*

Type of Application	(very) suitable	average	(absolutely) unsuitable
Internet Browsing	20.00%	25.45%	54.55%
Desktop Replacement	18.19%	18.18%	63.63%
Presentations	61.82%	27.27%	10.91%
Entertainment	67.27%	12.73%	20.00%
Traffic Information	87.27%	9.09%	3.64%
Advertising	83.64%	7.27%	9.09%

Based on the aforementioned scenario, where the participants were asked to imagine the situation of being within an office hallway working on a large public display, we asked the participants how comfortable they would feel, using such a large display in the described situation. Less than 10% stated that they would feel comfortable or even very comfortable (see Table 10).

Table 10: *Answers to the question "Would you feel comfortable using a large public display in an office hallway in general?", rated on a scale from 1 (very comfortable) to 5 (absolutely uncomfortable).*

1	2	3	4	5	Total	Mean	Variance	Std. Error
2	3	21	14	15	55	3.67	1.0929	1.0454
3.64%	5.45%	38.18%	25.45%	27.27%	100.00%			

We further asked them whether they would use the large display for viewing e-mails or documents of private content (e.g., an e-mail from a family member). The question had to be rated from 1 (yes, always) to 5 (no, never). The result was very distinct, but not yet surprising: almost all participants would rather not use a large public display for viewing private content.

Table 11: *Answers to the question "Would you use the large display for viewing private content?", rated on a scale from 1 (yes, always) to 5 (no, never).*

1	2	3	4	5	Total	Mean	Variance	Std. Error
0	0	1	11	43	55	4.76	0.2169	0.4657
0.00%	0.00%	1.82%	20.00%	78.18%	100.00%			

Finally, we asked the participants to consider the case in which they have to immediately send an urgent e-mail of private nature. In the described scenario, the large display is right next to them, compared to their own office, which is a few minutes away. The question was, whether they would prefer to use the large public display or rather go back to their private desktop computer instead.

Table 12: *Answers to the question "If you need to send an urgent e-mail, would you rather go back to your desktop computer or use the large display (that happens to be spatially close to you)?".*

Use Large Display	Go Back	Total
12	43	55
21.82%	78.18%	100.00%

Almost 80% would rather go all the way back to their desktop computer instead of using the public computer system directly next to them. The fact that a *private* e-Mail needs to be sent certainly is the main reason for this result. Furthermore, it is worth mentioning that the answer depended on the *technical experience*: while only less than 8% of the *very experienced* users would use the large display, more than 23% of the users that are *not very experienced* and 28% of the users that have *no experience* would use the large display.

Table 13: *Answers to the question "How important is privacy to you in general?", rated on a scale from 1 (very important) to 5 (not important at all).*

1	2	3	4	5	Total	Mean	Variance	Std. Error
29	24	1	0	1	55	1.55	0.5025	0.7089
52.73%	43.64%	1.82%	0.00%	1.82%	100.00%			

In this context, we asked the participants how important privacy was to them in general. Similar to the scales before, the participants could express their preferences on a scale from 1 (very important) to 5 (not at all important). Again, the results were not really surprising as almost all participants considered privacy to be important or very important (see Table 13).

Summing up the results, the evaluation showed that users are largely concerned with their privacy and that they are rather reluctant to use large public displays, at least without proper protection against possible privacy infringements.

In the last part of the evaluation, we extended the initial scenario and asked the participants to imagine that there would be "some kind" of privacy protection system available that is able to protect their privacy by hiding private or sensitive content whenever other people approach the large public display. In the first part of this second questionnaire we explicitly requested them to disregard *how* the system works. We then repeated the questions of whether they would feel generally comfortable with using the large public display (Table 14), and whether they would use the display for displaying public and private content (Table 15). The light bars stand for the answers if no privacy protection system is available while the dark bars represent the existence of such a system.

In case of public content, a system designed to prevent privacy infringement resulted in the frequency of participants willing to use a large public display to almost sextuple from 5.45% to 30.91% regarding answer 1 (yes, always).

Table 14: *Answers to the question "Would you use a large public display for viewing public information depending on whether a privacy protection system is available?", both rated on a scale from 1 (yes, always) to 5 (no, never).*

	1	2	3	4	5
no system	5.45%	34.55%	30.91%	10.91%	18.18%
system	30.91%	45.45%	10.91%	9.09%	3.64%

In the case of private content, the result is even more obvious and distinct: while almost 80% of the participants answered that they would never (answer *5*) use a large display for viewing private documents without a privacy protection system, this number shrunk to 20% given such a system.

Table 15: *Answers to the question "Would you use a large public display for viewing private information depending on whether a privacy protection system is available?", both rated on a scale from 1 (yes, always) to 5 (no, never).*

	1	2	3	4	5
no system	0.00%	0.00%	1.82%	20.00%	78.18%
system	5.45%	20.00%	27.27%	27.27%	20.00%

Summarizing the results, it is evident that the provision of a privacy protection system can significantly increase the users' trust when using a large display in public environments.

3 Active Privacy Support for Large Public Displays

The insights gained in the previous evaluations were used to design a system for automated privacy support at large public displays. The developed application gives users the freedom to spontaneously work on large public displays, without the fear of privacy infringements through passers-by. The system automatically controls the information that is visible to others, without requiring users to employ any additional equipment. This is achieved by providing users with a "personal space" in front of large displays in a shared environment. Within that personal space, the information that is visible to others is automatically controlled according to the user's individual preferences. In order to adapt the information representation to the current context, people entering the private space around a public display are automatically detected and identified using infrared (IR) and radio frequency identification (RFID) technology. Based on the identity of the person entering the private space and the privacy preferences of the user working at the public display, the information currently visible is automatically adapted. Before the technical realization of the system is presented, the key ideas, which guided the conceptual design process, are illustrated.

3.1 Personal Space Concept

The desire for a personal space that is not penetrated by others is one of the most basic human rights and it has become even more important within the last decades. This tendency is reflected in our society by increasing privacy concerns regarding current and future information and communication technologies (see, e.g., Lahlou et al., 2005; McCarthy et al., 2004; Palen & Dourish, 2003). Clarke (1999) defines this desire as "the interest that individuals have in sustaining a personal space, free from interference by other people". In this contribution, this real-world concept is adapted to the virtual domain. The term 'personal space' refers to the space in which all interactions are only visible to the interacting user. Or, from another perspective, being outside this specific private space does not allow another person to see the content and nature of the interaction taking place.

Figure 1 illustrates the aforementioned concept of a personal space. The left picture shows a user working on a large display in a public space. The semicircle in front of the display shows the user's personal space. In this example, the personal space represents exactly the physical space that is necessary to remain free of interruptions or intrusions. As this space is currently not invaded by other users, all content is being displayed. The black areas on the display represent applications or documents with confidential content, the grey areas indicate applications with public information. On the right picture another person is entering the personal space. As this person might threaten the information privacy of the user working at the display, the confidential content (black outline) is temporarily concealed, while the public information (grey) is still visible.

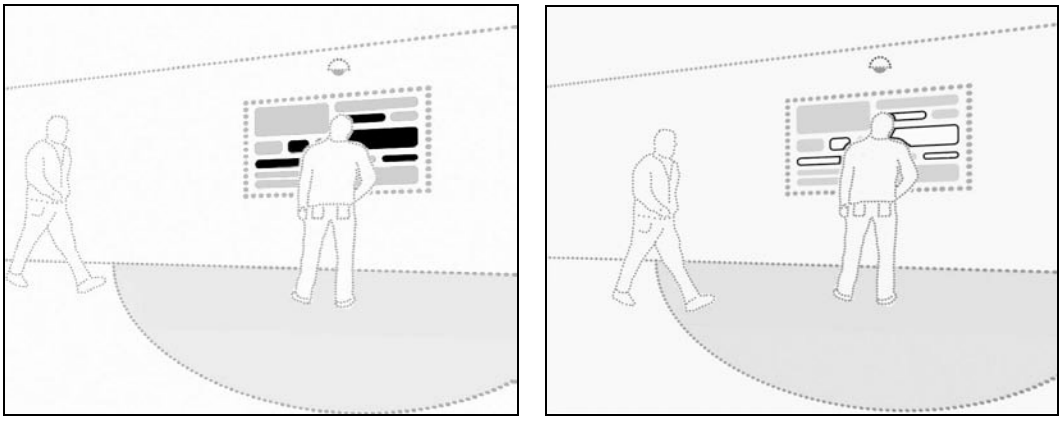

Figure 1: *Personal space around a public display (left), confidential information is hidden as soon as another person invades the personal space (right).*

3.2 Context-Adapted Privacy Protection

As pointed out before, most users are not willing to share private information with colleagues. The problem encountered here is that information cannot be classified as being public or private in general. How confidential a certain type of information is primarily depends on the individual assessment of each user. For example, Palen (1999) found, that information regarded totally innocuous by some users, were considered personally private by others. In the same way, Zhao and Stasko (2002) argue that individuals usually have different comfort zones in the level of personal information being broadcasted and that these comfort zones change over time. They conclude that individuals should be allowed to select the level of information about them that is being transmitted. But privacy settings not only depend on the sender's preferences, they are also determined by the identity of the information receiver. The behavior regarding the disclosure of personal information in multi-user situations was investigated in various studies (see, e.g., Röcker, 2006 or Olson et al., 2005). All studies came to the result, that the willingness to provide information varies widely with the type of information and the information receiver.

3.3 Privacy Levels to Control Information

In real-world situations, the disclosure of personal information is usually done in an ad-hoc manner and often does not follow any strict rules. But when using an automated privacy protection system, the disclosure of personal information has to follow a basic concept with specific „rules". As illustrated before, users have different preferences depending on what they are doing and to whom they are providing certain information. Hence, the adaptation of the displayed information must depend on the content of the application or document as well as on the person(s) invading the personal space. But using individual privacy settings for each situation would require that all persons, documents and applications have to be classified beforehand.

3.3.1 *Group-Based Privacy Control*

Experiences with existing systems showed that individual classifications are not necessary to manage privacy in multi-user situations. In a study with N=36 users, Patil and Lai (2005) found a significant preference for defining privacy permissions at a group level. Around 70% of the participants chose to configure permissions in 'group mode', with significantly different permissions granted to the various groups. Based on the feedback gained by the participants, they conclude that utilizing grouping mechanisms provides the flexibility needed to appropriately manage the balance between privacy control and the burden of configuration. Results leading to similar design recommendations were found in studies by Olson et al. (2005) and Lederer et al. (2003).

3.3.2 Classification of Users

These findings led to the approach of using a group-based classification scheme, in which each individual is assigned to a specific 'privacy level'. Table 16 gives an example how privacy levels can be defined.

Table 16: *Example for Different Privacy Levels.*

Privacy Setting	**Description**
Level 1 (Private)	The highest privacy level covers the most private content and is meant for eyes of its owner only. This includes personal emails and private documents.
Level 2 (Partner)	The second privacy level includes all information that is meant for intimate circle of persons only. In this example, the user's partner is assumed to be trustworthier than everyone else.
Level 3 (Family)	This level contains all information that is family-internal and potentially accessible by all family members.
Level 4 (Friends)	Hides family-internal information (e.g., banking information), but still allows access to other personal information (e.g., pictures from the last holidays).
Level 5 (Public)	All applications containing personal or confidential information are hidden.

3.3.3 Classification of Documents and Applications

The classification of documents and applications is realized through a keyword system, which allows a high degree of flexibility. Every document and application can be assigned to one of the five privacy levels shown above. A keyword is a string that is searched for in the window title of a document or application. Figure 2 shows part of a screenshot taken from an application with an open document. The window title contains the name of the document ("Bank of America") and the name of the application ("Microsoft Internet Explorer").

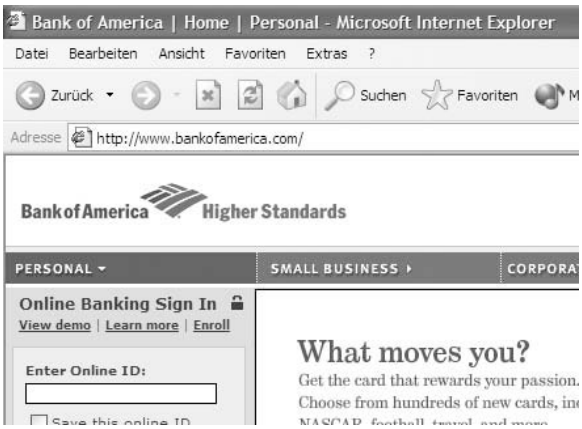

Figure 2: *Screenshot of an open application with several keywords in the title bar.*

Using the keyword system, a user can classify all websites accessed via the Internet Explorer to the highest privacy level (level 1) by adding the keyword 'Internet Explorer' to the keyword list of the first level. In addition, it is also possible to hide only specific websites. For example, adding the keywords "Bank of America" to the keyword list of the second level, results in all documents containing the keywords "Bank of America" being hidden from all users except for the persons assigned to the second level. In this case it is not important which application is used to access the document.

3.4 Measure to Preserve Privacy

As there is a natural trade-off between usability and the level of privacy protection, several protection measures were implemented. Currently, there are six possible actions available to users, each having its specific advantages and disadvantages:

Table 17: *Advantages and disadvantages of the different measures for privacy protection.*

Method	Advantages	Disadvantages
Privacy Protection De-Activated	No interference of ongoing activities	No privacy protection at all
Display Message	No interference of ongoing activities, but users are still aware of people entering their personal space	No automated privacy protection by the system, but user can manually hide specific content
Open Cover Window	All open windows remain in their position, adequate privacy protection since confidential data is visually blocked	Interference of current activities, all windows are still visible in the taskbar
Minimize Window	All open windows will appear in the same position as before, good privacy protection as confidential information is temporarily hidden	Interference of current activities, all windows are still visible in the taskbar
Hide Window	All open windows will appear in the same position as before, high privacy protection since they are temporarily hidden (even in the taskbar)	Interference of current activities
Close Window	Highest level of privacy, since all confidential applications and documents are closed	Interference of current activities, work is lost unless saved before

The settings for the different privacy levels are controlled using a graphical user interface, which enables users to adjust the levels to their individual preferences. The interface consists of two parts, the *Keyword Manager*, and the *Action Manager*.
The *Keyword Manager* comprises five keyword lists (corresponding to the five privacy levels), which can be individually adapted by the user. Furthermore, users can choose in which order the lists are checked, when a keyword is looked up. This concept enables users to express their general attitude towards sharing information. Users with a strong desire for privacy, who regard specific information as sensitive, unless expressed otherwise (e.g., by creating an exception rule), would choose to start the keyword search in the keyword list that represents privacy level 1 (private).
The *Action Manager* allows users to choose the action (as described in Table 17), which is taken in case of a keyword match. In addition, users can overrule the automatic comparison as well as the action taken for affected windows (e.g., windows that have one or more keywords in their title bar). By doing this, they can choose between "All Windows" and "Active Window". The option "All Windows" executes the selected action for every open window, regardless of the keywords in the title bar. "Active Window" affects only the currently active window (i.e., the window the user is currently working on).

4 Technical Realization of SPIROS

In order to implement the concept outlined in the previous section, we developed a privacy protection system called SPIROS (**S**ystem for **P**rivacy-Enhanced **I**nformation **R**epresentation in **O**pen **S**paces). Following the conceptual design approach, privacy protection is achieved in a three-step process:

- First, people entering the personal space of the user are detected and if possible identified.
- Second, the system determines and subsequently compares the privacy levels of the identified person(s) with the privacy levels of the currently open applications and documents.
- Third, the system initiates privacy-preserving measures according to the result of the comparison and the user's preferences.

The remainder of this section provides a detailed description of the underlying sensing infrastructure as well as the software architecture.

4.1 Sensing Infrastructure

The necessary information about nearby individuals is collected via a hybrid sensing infrastructure consisting of infrared sensors and RFID readers. People entering a personal space are detected by the infrared sensors and are simultaneously identified through the RFID system. All sensors are individually adjustable regarding their detection range and angle. This allows an adaptation of the user's personal space to the specific requirements of the environment.

4.1.1 *RFID Readers*

RFID is already widely used today (Fleisch & Mattern, 2005) and belongs to the basic sensor types available in most smart office environments. RFID technology enables contactless identification of people and objects that are equipped with a transponder. As RFID transponders are currently being integrated into a vast variety of everyday objects, it is assumed that users in smart office environments are not required to carry any additional RFID transponders in order to be identified. The SPIROS system was realized using an active RFID, which allows adjusting the reading ranges of the system to the spatial extension of the personal space. Hence, people carrying an RFID transponder are identified as soon as they enter the personal space around a public display.

4.1.2 IR Sensors

To detect the presence of persons who are not equipped with an RFID transponder, a special motion detection system was developed (see Figure 3). The system consists of several infrared detectors and a central communication unit, which can handle up to ten IR detectors simultaneously. The IR sensors are distributed in the environment and detect motion within a defined area. The communication unit aggregates the signals received from all IR sensors, and transmits them via a USB link to a host computer. Hence, if people approach the display, who can not be identified, it would be still possible to hide all personal information currently being displayed.

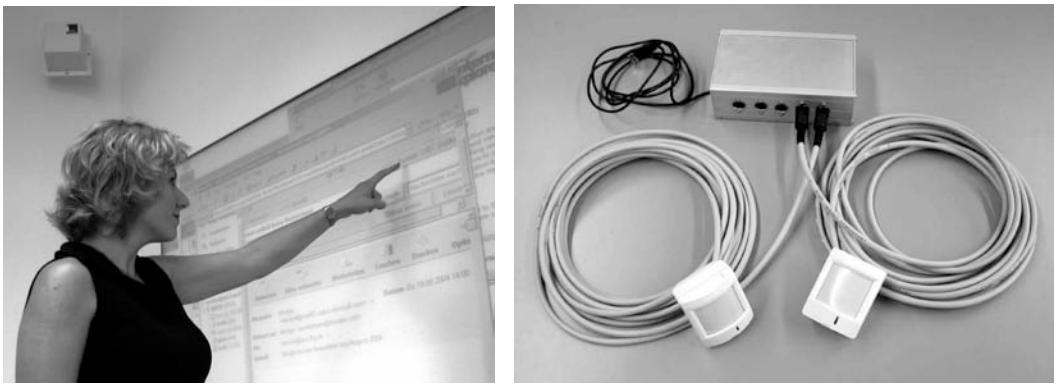

Figure 3: *Large public display with an RFID antenna in upper left corner (left) and infrared detection system with two sensors (right).*

4.2 SPIROS Architecture

The SPIROS architecture consists of three main components (see Figure 4):

- The *SPIROS Scanner Manager* (SSM), which identifies persons entering the personal space around the public display,
- The *SPIROS Privacy Manager* (SPM), which adapts the displayed information to the pre-defined user preferences and identified persons, and
- A database for storage and communication.

Figure 4: *General overview of the system.*

The separation of the SSM and SPM was done due to performance reasons. In addition, the separation allows several SSMs to run simultaneously, with each entity being responsible for one or more large public displays. This is of particular importance if several public displays are spatially distributed in an intelligent environment.

The main function of the SSM component is the identification of people who are within the reading ranges of the connected RFID readers. The IDs of all read RFID transponders are stored in the database. This data is then used by the SPM component. The SPM is responsible for adapting the displayed information to the user's privacy preferences and the persons currently present around the display. Whenever one of the IR sensors next to the display is triggered, the SPM retrieves the ID of the RFID transponders within the personal space and determines the privacy level of the corresponding person(s) as well as the privacy levels of the currently open windows. Based on this information, the content that is not supposed to be seen by the passers-by is temporarily hidden until the persons have left the personal space.

The following sections provide a more detailed description of the different SPIROS components and illustrate their general operating principles.

4.2.1 SPIROS Scanner Manager (SSM)

As mentioned before, the SSM operates the RFID readers and inserts all scanned tags within reading ranges of the system into the database (see below). Once the SSM has successfully connected to the RFID reader and the database, it starts polling the reader for RFID transponders in range. Whenever transponders are read by the reader, the SSM checks whether the transponders' IDs have already been inserted into the database. If this is not the case, the newly discovered ID is added to the database. The main problems encountered in the test phase were malfunctions due to missing or erroneous identification data. This happened, for example, if RFID transponders were not detected although they were within the reading range. To eliminate such problems, the SSM uses an internal counter for each transponder. As explained above, the ID of each detected transponder is inserted into the database. This entry is only removed if the transponder is not read for three consecutive reading cycles.

4.2.2 SPIROS Privacy Manager (SPM)

When the personal space of a user is invaded by other persons, the SPM hides confidential information according to the user's preferences. On starting, the SPM retrieves the user's profile from the database, creates a temporary table, and initiates the connection to the IR sensors using DirectX. The temporary table contains the user's current relationships to all other users. This is done by assigning the user's partner(s) to the '*partner level'*, family members to the '*family level'*, friends to the '*friends level'*, and all remaining users to the '*public level'*. Once the initialization phase has been completed, the SPM switches to the operating phase.

The SPM starts by checking an internal counter, which that is meant for undoing actions (e.g., windows that are minimized or hidden need to reappear). After each cycle, the counter is increased by one. If this counter reaches a certain limit, all actions taken before are reversed. In a second step, the SPM checks the IR sensors for activity. If any motion is detected, the counter is set back to zero. This is necessary in order to guarantee that all confidential information is hidden as long as other users are in close proximity to the display.

Based on the IDs of the detected transponders, the highest privacy level of all users within the personal space is calculated. In the same way, the privacy levels of the currently open windows are determined by scanning all window titles. To determine which windows should be hidden, the privacy levels of both, the passers-by and the active windows are compared. Depending on the user's pre-defined preferences, a specific action is initiated (see Table 17).

4.2.3 *SPIROS Database*

All information required by the SSM and SPM component is stored in a central database. The main table (*users*) contains the users' IDs as well as the individual privacy preferences. The privacy levels described in Table 16 are represented through the three tables *partners*, *family_members* and *friend*s, which contain information about the social relationships among users. If users are not contained in one of these three tables, they are assigned to privacy level five ('public'). To guarantee a quick look-up, a temporary table is created, that contains the user's current relationships to all other users. The keywords used for determining the privacy level of an active window are stored in five individual keyword tables. The IDs of detected RFID transponders are stored in the table *scanned_rfids*, and are then mapped to the table *users* by the table *temp*.

5 Evaluation of the Developed Prototype System

The SPIROS prototype application was tested in a third evaluation. Therefore, the developed system was presented to the same group of persons who already participated in the second study. This time, the participants were asked to rate the conceptual approach as well as the implemented

protection mechanisms regarding their appropriateness for daily usage and their usefulness to protect privacy. The first part of the questionnaire briefly described the developed system. It was explained that the system scans the environment and is able to detect people passing-by the display. It is further illustrated how users can classify documents and applications and assign special actions that will be executed by the system if other persons approach the display.
For a better understanding, a concrete situation was described in form of a scenario. The participants were asked to imagine a situation, were they are viewing a project-related document as well as a news page in an additional browser window. The project document contains information that only authorized people (in this case project members) are allowed to see. While they are browsing through the confidential project document, a person, who works in the same company, but is not a member of the project team, approaches the display. In this case, the presented system would be able to minimize or hide the project-related document, but leave the browser window open. Thus, the approaching colleague would see the news website, but not the confidential project information.
We first wanted to know, how comfortable the participants would feel using SPIROS compared to other approaches. Therefore, the participants were asked to rate the different approaches on a scale from 1 (very comfortable) to 5 (absolutely uncomfortable).

Table 18: *Answers to the question "How comfortable would you feel working on a large display in a public environment?", rated on a scale from 1 (very comfortable) to 5 (absolutely uncomfortable).*

	SPIROS	**Generic System**	**No System**
(very) suitable	52.73%	45.45%	9.09%
average	34.55%	34.55%	38.18%
(absolutely) unsuitable	12.72%	20.00%	52.73%

The results shown in Table 18 basically disclose two things. First, that there is a tremendous difference between having a privacy protection system or not. And second, that users feel more comfortable with the idea of using SPIROS than using other systems. The first premise is rather obvious: while the majority of the users would feel rather uncomfortable if no system was installed (answers 4 and 5), only 20% felt the same way if there is a system available. The second point is less obvious but still visible: comparing the statistic means and variances of each distribution, the observable differences demonstrate the superiority of SPIROS over other approaches (see Table 19).

Table 19: *Mean and Variance of the question "How comfortable would you feel working on a large display in a public environment?", rated on a scale from 1 (very comfortable) to 5 (absolutely uncomfortable).*

Type of Privacy Protection	***Mean***	***Variance***
No System	3.67	1.0929
Generic System	2.67	0.8747
SPIROS	2.42	0.8615

Thus, it is not surprising that the majority of users would prefer SPIROS. More than two third (67%) are willing to protect their privacy with SPIROS when asked whether they would use the system (see below). Very important was also the assessment of the possible measures that can be

taken by SPIROS. During the evaluation, we proposed four possible actions, which had to be rated on according to their appropriateness to protect privacy (see Table 20 for the results):

- "Show Message"
  (a pop-up message saying "someone is approaching" is displayed),
- "Cover Window"
  (a cover window with harmless content pops us and covers private or sensitive information),
- "Minimize Window"
  (all windows that currently display private or sensitive content are minimized), and
- "Hide Window"
  (completely hides all windows displaying sensitive content, i.e., they are not even visible in the task bar).

Table 20: *Answers to the question "What do you think of each possible action?", rated on a scale from 1 (very suitable) to 5 (absolutely unsuitable).*

	Hide Window	**Minimize Window**	**Cover Window**	**Display Message**
(very) suitable	69.09%	61.82%	50.90%	0.4182
average	20.00%	16.36%	30.91%	0.2364
(absolutely) unsuitable	10.91%	21.82%	18.19%	0.3454

We were rather curious to find out which action would be preferred to protect visual privacy at public displays. The feedback on displaying a message was relatively balanced: obviously, people see this action very differently. The other three actions received a better feedback: more than 50% considered the cover window to be good or very good, more than 60% thought the same of minimizing, and early 70% found hiding to be good or very good. Apparently, hiding private or confidential information seems to be the preferable solution for most of the participants. Finally, we wanted to know whether the participants would generally use SPIROS (see Table 21). Looking at the previous results, it is not surprising that the majority of participants would use SPIROS: more than two third (67%) are willing to protect their privacy with the described system.

Table 21: *Answers to the question "Would you use such a system?".*

Yes	***No***	***Total***
37	18	55
67.27%	32.73%	100.00%

6 Conclusion

In this chapter we presented a novel concept for personalized privacy support on large public displays. In a first step, two formative evaluations were conducted in order to analyze the requirements of potential users regarding the protection of private information on large public displays. The insights gained in these evaluations were used to design a system that automatically adapts the information visible on public displays according to the current social situation and the individual privacy preferences of the user working on the display. In a third evaluation, the developed system was evaluated regarding its appropriateness for daily usage and its usefulness to protect privacy. The results of the evaluation showed that users are in general willing to trust system-based protection mechanisms, provided that they are well implemented. In this context, the

proposed combination of pre-defined privacy profiles and context-adapted information visualization proved to be a good trade-off between usability and adequate privacy protection.

7 References

Bellotti, V., & Edwards, K. (2001). Intelligibility and Accountability: Human Considerations in Context Aware Systems. In: *Human-Computer Interaction,* Special Issue on Context-Aware Computing, 16(2, 3 & 4), pp. 193 – 212

Berger, S., Kjeldsen, R., Narayanaswami, C., Pinhanez, C., Podlaseck, M., & Raghunath, M. (2005). Using Symbiotic Displays to View Sensitive Information in Public. In: *Proceedings of the International Conference on Pervasive Computing and Communications* (PerCom'05), Kauai Island, HI, USA, pp. 139 – 148.

Churchill, E. F., Nelson, L., Denoue, L., Helfman, J., & Murphy, P. (2004). Interactive Systems in Public Places: Sharing Multimedia Content with Interactive Public Displays: A Case Study. In: *Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, pp. 7 – 16.

Clarke, R. (1999). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Retrieved January 13, 2006, from http://www.anu.edu.au/people/Roger.Clarke /DV/Intro.html

Eaddy, M., Blasko, G., Babcock, J., & Feiner, S. (2004). My Own Private Kiosk: Privacy-Preserving Public Displays. In: *Proceedings of the International Symposium on Wearable Computers* (ISWC'04), pp. 132 – 135.

Eldridge, M., Barnard, P., & Bekerian, D. (1994). Autobiographical memory and Daily Schemes at Work. In: *Memory,* 2(1), pp. 51 – 74.

Fleisch, E., & Mattern, F. (Eds.). (2005). *Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen*. Heidelberg, Germany: Springer-Verlag.

Greenberg, S., Boyle, M., & LaBerge, J. (1999). PDAs and Shared Public Displays: Making Personal Information Public, and Public Information Personal. In: *Personal Technologies*, 3(1), pp. 54 – 64.

Huang, E. M., & Mynatt, E. D. (2003). Semi-Public Displays for Small, Co-located Groups. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'03), pp. 49 – 56.

Huang, E. M., Russell, D. M., & Sue, A. E. (2004). IM Here: Public Instant Messaging on Large, Shared Displays for Workgroup Interactions. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'04), pp. 279 – 286.

Lahlou, S., Langheinrich, M., & Röcker, C. (2005). Privacy and Trust Issues with Invisible Computers. In: *Communications of the ACM*, 48(3), pp. 59 – 60.

Lamming, M., Eldridge, M., Flynn, M., Jones, C., & Pendlebury, D. (2000). Satchel: Providing Access to Any Document, Any Time, Anywhere. In: *ACM Transactions on Computer-Human Interaction*, 7(3), pp. 322 – 352.

Langheinrich, M. (2001). Privacy by Design – Principles of Privacy Aware Ubiquitous Systems. In: *Proceedings of the 3rd International Conference on Ubiquitous Computing* (Ubicomp'01), September 2001, Atlanta, USA, pp. 273 – 291.

Lederer, S., Dey, A., & Mankoff, J. (2003). Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'03), Ft. Lauderdale, USA, pp. 724 – 725.

McCarthy, J. F., McDonald, D. W., Soroczak, S., Nguyen, D. H., & Rashid, A. M. (2004). Augmenting the Social Space of an Academic Conference. In: *Proceedings of the ACM Conference on Computer Supported Cooperative Work* (CSCW'04), Chicago, Illinois, USA, pp. 39 – 48.

Needham, B. H., & Koizumi, D. H. (1998). *Method of Displaying Private Data to Collocated Users*, US Patent 5,963,371.

Olson, J. S., Grudin, J., & Horvitz, E. (2005). A Study of Preferences for Sharing and Privacy. In: *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems* (CHI'05), pp. 1985 – 1988.

Palen, L. (1999). Social, Individual and Technological Issues for Groupware Calendar Systems. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'99), pp. 17 – 24.

Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'03), Ft. Lauderdale, Florida, USA, pp. 129 – 136.

Patil, S., & Lai, J. (2005). Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'05), pp. 101 – 110.

Rekimoto, J. (1998). A Multiple Device Approach for Supporting Whiteboard-based Interactions. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'98), pp. 18 – 23.

Röcker, C. (2006*). Awareness and Informal Communication in Smart Office Environments.* Verlag Dr. Driesen, Taunusstein, Germany. ISBN 3-936328-65-X.

Russell, D. M., & Gossweiler, R. (2001). On the Design of Personal & Communal Large Information Scale Appliances. In: *Proceedings of the International Conference on Ubiquitous Computing* (UbiComp'01), pp. 354 – 361.

Shoemaker, G. B. D, & Inkpen, K. M. (2001) Single Display Privacyware: Augmenting public displays with private information. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'01), pp. 522 – 529.

Whittaker, S., Frohlich, D., & Daly-Jones, O. (1994). Informal workplace communication - What is it like and how might we support it? In: *Proceedings of the ACM Conference on Human Factors in Computing Science* (CHI '95). ACM, NY, pp. 131 – 137.

Yerazunis, W. S., & Carbone, M. (2002) Privacy-Enhanced Displays by Time-Masking Images, *Technical Report TR2002-011*, Mitsubishi Electric Research Laboratories.

Zhao, Q. A., & Stasko, J. T. (2002) What's Happening?: Promoting Community Awareness Through Opportunistic Peripheral Interfaces. In: *Proceedings of the Conference on Advanced Visual Interfaces* (AVI'02), pp. 69 – 74.