Privacy and User Trust in Context-Aware Systems

Saskia Koldijk[1,2], Gijs Koot[1], Mark Neerincx[1,3], Wessel Kraaij[1,2]

[1] TNO, The Netherlands, {name.surname}@tno.nl
[2] Radboud University Nijmegen, The Netherlands
[3] Technical University Delft, The Netherlands

Abstract. Context-aware systems (CAS) that collect personal information are a general trend. This leads to several privacy considerations, which we outline in this paper. We present as use-case the SWELL system, which collects information from various contextual sensors to provide support for well-being at work. We address privacy from two perspectives: 1) the development point of view, in which we describe how to apply 'privacy by design', and 2) a user study, in which we found that providing detailed information on data collection and privacy by design had a positive effect on trust in our CAS. We also found that the attitude towards using our CAS was related to personal motivation, and not related to perceived privacy and trust in our system. This may stress the importance of implementing privacy by design to protect the privacy of the user.

Keywords: Context-aware systems, privacy by design, user evaluation, trust.

1 Introduction

Advances in sensing, the rise of smartphones and mobile internet, together with trends such as personalization have led to both demand and possibilities in the area of context-aware systems (CAS) and such applications are now very common. Context-awareness for applications has been broadly defined as the use of environmental elements by applications to personalize their service for the user [1]. A simple example is given by a navigation application: you tell the application where you want to go, the explicit data, while the application obtains your current location from the mobile device, which is then the contextual data.

As the scale and application of data collection increase, privacy concerns are rising over the new worlds of possibilities that are revealed by data scientists. Privacy has been defined as the "boundary control process in which individuals regulate when, how, and to what extent information about them is communicated to others" (p. 21) [2]. There often seems to be a trade-off for users between using a service and their privacy: they can use a better personalized and contextualized service by providing more context information, often with the cost of losing control over their personal (context) data. [3] states that "Businesses inevitably collect and use more and more personal data, and while consumers realize many benefits in exchange, there is little doubt that businesses, not consumers, control the market in personal data with their own interests in mind." (p.1). In [4] this problem is described as an 'asymmetry of information' in which the data collector knows much more about how the data will be used than the data owner, who has no control. This has led to debates about consumers' privacy and privacy legislation.

In this research we want to investigate how to address privacy in CAS and whether information on privacy has a positive impact on users' trust and attitude towards using the system. In [5] the authors found that in social networks, privacy and security had an effect on the user's trust in a system and the attitude towards the system, which in turn influenced the intention to use the system. An overview paper [6] outlines that firms can build trust by implementing fair information practices, communicating a privacy policy explicitly and/or using privacy notices and seals of approval.

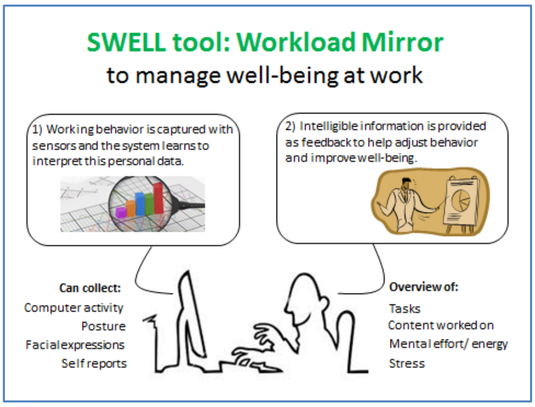
We first analyze which privacy aspects are of particular interest in CAS by doing a Privacy Impact Assessment. We make use of a use-case called SWELL, in which work related behavior data is collected with sensors, to provide personalized feedback and support for well-being at work. As the collected data may include rather personal information (e.g. content worked on or facial expressions), interesting privacy aspects arise. This domain distinguishes our research from related research in which privacy is often investigated in context of social networks, user profiling, e-commerce, marketing or mobile location enhanced technologies [6]. We then outline how Privacy by Design [10] can be applied in CAS, resulting in some simple guidelines for developing privacy-friendly CAS. There are many papers on principles for privacy by design, but empirical studies are sparse. Therefore we performed a user study to investigate the effects of privacy by design on users. Our method is similar to the one used in a study on privacy concerns in location-based mobile services [7]: users were presented our envisioned system and were asked to give ratings. Our hypothesis is that when users have access to detailed information on data collection and privacy by design, the transparency of the system is higher and users have less privacy concerns and more trust in the system. As a consequence, we hypothesize, they have a more positive attitude towards using the CAS.

In the remainder of this paper we first introduce our use-case (Section 2). Then we present important privacy aspects (Section 3). In Section 4, we describe how privacy by design can be applied. We then present results of our user study (Section 5). We end with a Discussion (Section 6) and Conclusion (Section 7).

2 Context aware system use-case: SWELL

In this section we present a use-case from the project SWELL[1] to apply our analyses regarding privacy to. The SWELL system makes use of a variety of contextual sensors, which makes it interesting for analyzing associated privacy issues. We first outline the CAS and then present a scenario.

[1] www.commit-nl.nl/projects/swell-smart-reasoning-systems-for-well-being-at-work-and-at-home



SWELL tool: Workload Mirror
to manage well-being at work

1) Working behavior is captured with sensors and the system learns to interpret this personal data.

2) Intelligible information is provided as feedback to help adjust behavior and improve well-being.

Fig. 1. Information about the SWELL system.

SWELL Workload Mirror. The SWELL Workload Mirror is a CAS under current development that provides information about working behavior to help employees reach more well-being at work [8]. Knowledge workers often experience stress building up, which in the worst case results in burn-out. We think that helping knowledge workers to become more aware of what makes them feel stressed, can help them handle and avoid stress. The SWELL system senses data about an user's environment with unobtrusive sensors, combined with occasional self-reporting by the user. Smart reasoning algorithms extract the recent context and mental state from this data. The system is aimed at helping users to reach their well-being goals by providing information, feedback and support.

SWELL scenario. Bob is 40 years old and works in an office from 9 to 5, where he performs knowledge work. Since some time now, Bob feels some tension and finds it hard to get work off his mind in the evenings. At the end of his working day he often notices that he has not completed all planned tasks and he feels stressed.

Bob decides to use the SWELL system (see Figure 1). At the end of his working day he opens the SWELL Workload Mirror to look back at his day. He sees an overview of the tasks he performed and content he worked on, combined with information on his subjective energy level. He notices that he worked very fragmented which probably caused his loss of overview and decline in energy. Bob decides that it would be better for him to stay focused on his planned work and determine a timeslot to do all ad-hoc tasks. He enables a functionality of the SWELL tool, which warns him when he makes too many task switches again. Bob also notices that, in fact, he has done a lot of useful things today and can go home satisfied.

3 Privacy aspects

To analyse the potential privacy risks around collecting personal data with the SWELL system, we performed a Privacy Impact Assessment (PIA). As [9] describes it: “PIAs provide a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments in the development of a new technology, service or product.” (p. 54). We went through the PIA question catalogue[2] and in this section we present the resulting main privacy considerations and provide the most important PIA suggestions to build a privacy-friendly CAS.

- *Goal of data collection*: We found that it is very important to clearly describe the goal for which the data is collected. Only when users understand what the system does and why the collection of data is necessary, they will be able to take a well informed decision on how to use the system.
- *Type of data*: The PIA highlighted that the type of data should be suitable to fulfil the goal. Do not collect more data than necessary. Be aware that the combination of different sorts of data can be even more privacy sensitive. Store data as aggregated as possible, for example only store summaries of facial expressions instead of video. Time limit the storage of personal data. This prevents function creep, i.e. using the data for other purposes. In any case, identifiers such as full names and email-addresses should be avoided where possible.
- *Reactions to the system*: In the PIA it was pointed out that you should be aware that reactions to new innovative systems are hard to predict. The data that you want to collect can be sensitive, for example when you collect data on geo-location or work performance. Prevent reputational damage. The right story and suitable introduction will be essential to make the tool a success. There is a risk that people involved do not want to participate. For users who do not want to use e.g. a camera an alternative means to get the necessary information should be provided, e.g. let users input their mood themselves.
- *User control*: In the PIA it was recommended to let the user be in control of the system and the settings. You should tell the user which data is collected and (if applicable) who will have access to this data. Their permission should be given based on a free and well informed decision. Giving information on what is done with the data also contributes to transparency and evokes trust. Users have the right to see their own data and may request removal of data.
- *Quality of the data*: The PIA highlighted that it is important to pay attention to the quality of the data. The data should be up-to-date, correct and complete. Depending on the sensor, the data can be more accurate (e.g. computer logging) or less accurate (e.g. facial expressions from video analysis). You can reach better quality by for example letting the user check, correct or update the data. Be aware of consequences of using wrong data.
- *Security of the data*: Security of the data is a must. In the PIA it was recommended to set up a data security plan to establish which security actions are taken to guarantee suitable protection of the data. Prevent unwanted or unauthorized access of the data. Take the sensitivity of your specific data into account.

[2] developed by Norea: http://www.norea.nl/Norea/Actueel/Nieuws/Presentatie+PIA.aspx

- *Data responsibilities*: The PIA pointed out that the more parties are involved, the higher the risk of data getting lost, unclear responsibilities or use of data for other purposes. Take care that all parties handle the data carefully. Make a clear data description and a clear description of tasks and responsibilities. Make clear who has to take the measures necessary to prevent risks.
- *Data sharing*: We found that in case of data sharing, you should take care that the user gives consent and that the data is used in the intended way. Data can be shared in several ways. First of all data may be shared between users, when it is the wish of the specific user to share data for a personal goal or benefit. Second of all, data may be shared for improving the system, e.g. to train underlying models with all users' data. Thorough analysis should be done whether no personal information could leak in this way. Finally, it may be interesting to share collected datasets with the research community. When data is distributed you should describe the data well and take care that the distribution of data is in line with the expectations of the users involved. Make a clear data description document. Pay attention to purpose limitation and risks resulting from combining data from different sources.

Being aware of these points of interest at an early stage of design should enable developers to implement privacy into their context aware system.

4 Privacy by Design

In this section we present how the outlined privacy aspects for the SWELL use-case can be addressed from the developers perspective by using Privacy by Design [10]. We describe how 8 Privacy Design Strategies [11] can be applied to develop a context aware system that follows current privacy legislation. We also give some tips on specific Privacy Design Patterns that can be used to implement each strategy. For a more elaborate description and specific references refer to [12].

- First of all it is important to **INFORM** the user about the goal of the system and the data that will be collected for this aim. You should always use *Informed Consent*, which means that the you get permission from the user to collect data for a specified purpose. You can also provide the user a *Privacy Dashboard,* such that the user has an overview over his privacy settings.
- Moreover, it is important to give the user **CONTROL** over the data and what is done with it. There are different ways to let users feel in control. Information helps users to understand the system and power allows them to decide which data is collected, how it is used and with whom shared. Offering *Privacy Choices* helps to give them a feeling of control and a system that is easy to use also increases the perceived control.
- The task of the designer of the system is it to **MINIMIZE** the amount of data that the system stores. This can be accomplished by selecting only the most relevant features (e.g. storing facial expression features instead of raw video recordings). In any case it is a good idea to only use *Pseudonyms* as identifiers, instead of storing data together with the users' real names. Furthermore, take care of good *Anony-*

mization. Even when you do not store the user's name, the unique combination of e.g. age and GPS location can make a user of the system identifiable. Prevent having identifiable entries and use *k-anonymity*. This means making at least k entries identical, for example by aggregating "age = 22" to "age = 20 to 30".

- By applying reasoning the data can often be **AGGREGATED** even further. Instead of detailed features, inferred information can be stored (e.g. whether someone experienced stress or not, instead of all facial expressions). You can for example *Aggregate Data over Time*, e.g. the main application of the last 5 minutes or the main facial expression. This also lessons the amount of data the system has to handle. Moreover you can also *Blur Personal Data*. This means you provide personal data only in a detail that is necessary and blur the rest, e.g. store location information not as a coordinates, but as a city name.
- The developer should take care to **HIDE** personal information, such that the data strictly belongs to the user and cannot be seen by others. When a user or application wants to access the data, *Authentication* should be used to ensure that no unauthorized access to the data takes place. To ensure the security of the data it is a good idea to *Store Data Encrypted*. You should encrypt the data locally on the users device and then send it over a secure connection to the cloud for storage. When the aim is to publish (parts of) the data one could apply *Sampling*. Instead of releasing all data a sample is drawn for releasing on the (public) cloud.
- Moreover it might be useful to **SEPARATE** different sorts of data. Storing data from different individuals at separate locations is called *Horizontal Data Separation*, while storing features in separated locations is called *Vertical Data Separation*. When handling privacy sensitive data it is also good to apply *Decentralization* and store (parts of the) data only locally, on the user's device.
- The system should be able to **ENFORCE** and **DEMONSTRATE** that it fulfils current legislation around privacy. You might want to use *Sticky Policies*, especially when sharing data. This means that you store alongside with your data its privacy policy for handling this data. In this way you prevent wrong use by 3rd parties.

By applying these 8 Privacy Design Strategies in the development of a CAS the resulting system will be privacy-friendly by design, adhering to current legislation.

5 User perspective: Evaluation study

Now we have seen how privacy can be addressed in the development of a CAS, we want to evaluate what effect giving information on privacy by design has on users. Our hypothesis is that when users are better informed about the data collection and privacy by design, the transparency of the system is higher and users have less privacy concerns and more trust in the system. As a consequence they have a more positive attitude towards using the system (see Figure 2 for our expected model). We also think personal characteristics play an important role. General privacy concerns might have an influence on perceived privacy and trust in a new system. Personal motivation might have an influence on attitudes towards use of the system. In the remainder of this section we outline how we tested our hypotheses in a user study with a mock-up of our SWELL tool.

5.1 Method

Participants. 124 people participated in our user study, 60% male, with an average age of 38 (SD = 10.6). Colleagues from other TNO departments (technical and behavioural sciences) were invited as participants, as they are knowledge workers and potential users of the SWELL tool to improve well-being at work. On a scale from 1-7 our participants scored on average slightly positive on well-being (4.7, SD = 1.2) and slightly positive on the item 'I want help to improve well-being' (*Motivation*) (4.9, SD = 1.7). Moreover, they scored on average neutral on *Privacy concerns* (4.1, SD = 1.5).

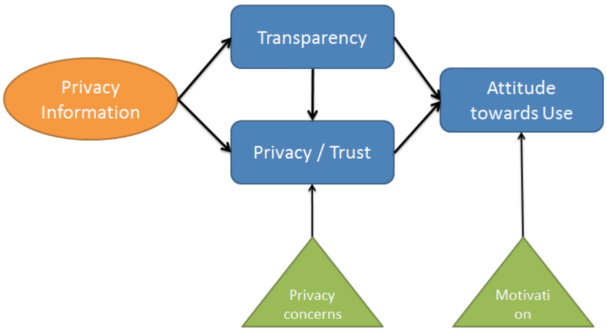
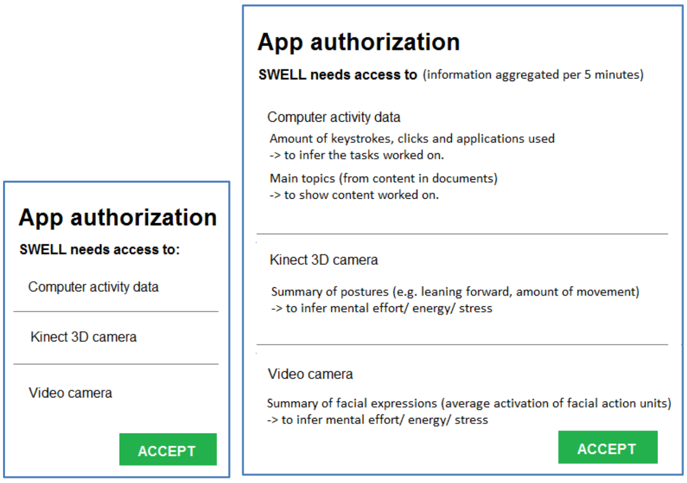


Fig. 2. Expected model. We manipulated whether participants had access to extra *Privacy Information*. Our 3 dependent variables are *Transparency* of the SWELL tool, attitudes regarding *Privacy and Trust*, and *Intention to Use* the SWELL tool. We expect that also personal characteristics (*Privacy concerns* and *Motivation*) play a role.



App authorization

SWELL needs access to:

Computer activity data

Kinect 3D camera

Video camera

App authorization

SWELL needs access to (information aggregated per 5 minutes)

Computer activity data

Amount of keystrokes, clicks and applications used
-> to infer the tasks worked on.

Main topics (from content in documents)
-> to show content worked on.

Kinect 3D camera

Summary of postures (e.g. leaning forward, amount of movement)
-> to infer mental effort/ energy/ stress

Video camera

Summary of facial expressions (average activation of facial action units)
-> to infer mental effort/ energy/ stress

Fig. 3. Mock-up of the access rights dialogue. Left: Control condition, right: Privacy condition.

Design. We manipulated whether the participants did or did not get extra information on data collection and privacy by design. Our experiment had thus a between-subject design and our independent variable is ‘privacy information’ (no, yes).

Procedure. An email was sent out to various TNO departments. By clicking a link, the participant was randomly assigned to the condition with or without privacy information and shown a website. On this website, first a short presentation was shown, either with or without slides on privacy. Both groups were then asked to fill in the same questionnaire.

Materials. *Presentation.* The first 7 slides were the same for both groups and presented a scenario for the SWELL Workload Mirror (see Section 2). Both groups were told that the goal of the SWELL tool is to support self-management of stress and that the users could enable or disable functionalities as they wish, such that the SWELL tool optimally supports them with functionality that they desire (e.g. sharing information with others).

The privacy group got to see extended information on the data that the system would collect (see Figure 3). Moreover, an additional slide gave them the following information on privacy by design:

- *Purpose limitation*: The collected data is only used for giving yourself insights to enable self-management.
- *Control*: You can enable or disable the computer logging, camera or Kinect sensors.
- *Data minimization*: The tool only processes data that is necessary to provide the functionality that you desire, e.g. the tool will use document content only when you want an overview of topics worked on.
- *Data aggregation*: The sensor data is processed locally on your device. Only summary information, like topics, average posture or facial expression, is stored – no keystrokes or video.
- *Adequate protection*: Your data is hidden from unauthorized access.
- *Data subjects right*: You have full control over your data, can view or delete it.

Questionnaire. The questionnaire had items on the following main categories: transparency of the SWELL tool, perceived privacy and trust, and attitudes towards use of the SWELL tool (see Table 1, items partly adapted from [5]). Besides these main items of interest, we added some items on personal characteristics. We used 7-point Likert scales (1 = ‘not’ to 7 = ‘very much’).

Dependent variables. To determine the main underlying concepts of the questionnaire items, we performed a factor analysis (PCA, see Table 1). We found 3 main underlying components, which represent: '*Transparency*', '*Privacy/ Trust*' [3] and '*Attitude towards Use*'. To test the reliability of each scale, we calculated Cronbachs' alpha (coefficient of internal consistency) for each set of items. As for all 3 scales alpha was high enough (> .6), we computed sum scores of the sets of items and averaged them to yield 3 main dependent variables.

Table 1. Questionnaire items (** item adapted from [5]*), loadings on PCA components (with Varimax rotation), and Cronbachs' alpha for combining these items to one concept.

Questionnaire item	C 1	C 2	C 3	Concept	α
I would trust SWELL to protect my privacy. *	**.862**	.176	.173	*Privacy/ Trust*	.884
I am confident that the information I provide will be secure. *	**.861**	.144	.105		
(reversed) I am concerned that the information I collect could be misused. *	**.832**	-.049	-.055		
(reversed) I believe inappropriate parties may view the information I provide. *	**.795**	-.022	-.048		
The SWELL tool is a trustworthy system.*	**.696**	.202	.236		
I feel in control of my personal data.	**.645**	-.027	.481		
The thought of using the SWELL tool is appealing to me. *	.071	**.923**	.053	*Attitude towards Use*	.890
I think using a computer system like SWELL could help me improve my well-being at work.	.013	**.834**	-.020		
I have positive feelings towards the SWELL tool in general.*	.231	**.802**	.127		
I think benefits of using the SWELL tool outweigh potential costs (effort, time).	-.052	**.795**	.027		
I want to use the SWELL tool.	.104	**.783**	.038		
I understand which information will be collected using the SWELL tool.	.146	.022	**.836**	*Trans-parency*	.655
It is clear to me how the SWELL tool works.	.050	.102	**.830**		
My current level of well-being at work (e.g. feeling in control, productive, energetic) is...				Personal characteristics	
I want help to improve my well-being.					
In general, I would say I am concerned about my privacy.					

5.2 Results

Personal characteristics. As we think personal characteristics may have an important influence on our dependent variables, we calculated Pearson correlations to check for these dependencies. We found a significant moderate correlation between *Privacy Concerns* in general and perceived *Privacy/ Trust* (r = -.548, p < .001). People who in general have many privacy concerns tend to score low on perceived privacy and trust regarding the SWELL tool. Furthermore, we found a significant weak correlation between the level of well-being and the desire to improve well-being (r = -.337, p < .001), as well as a significant moderate correlation between the desire to improve

[3] Items on perceived privacy and trust (from Shin, 2010) seemed to all load on one component. Therefore they are not further distinguished in our analyses.

well-being and *Attitude towards Use* of the SWELL tool (r = .457, p < .001). This means that people with low well-being want to improve well-being more, and people who want to improve well-being more have a more positive attitudes towards using the SWELL tool. In the remaining analyses we will use these personal characteristics as covariates.

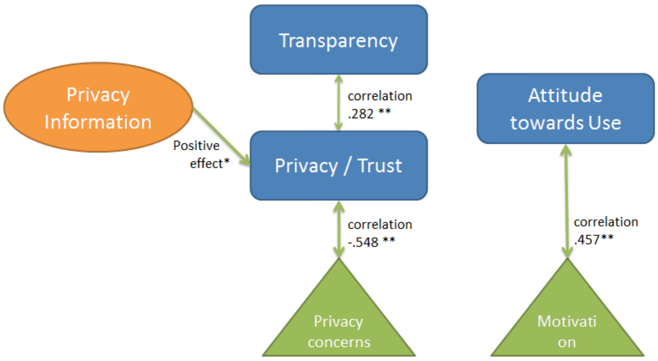


Fig. 4. Results. Influence of privacy information was analysed with ANOVA's. Relations among variables were analysed with Pearson correlations. (** significant on the .05 level, ** significant at the 0.01 level*).

Effects of privacy information. We were interested in whether giving extra information on data collection and privacy by design would have a positive impact on *Transparency* of the SWELL tool, attitudes regarding *Privacy and Trust*, and finally on *Attitude towards Use* of the SWELL tool (see Figure 3 for our expected model). Therefore, we performed an ANOVA with privacy information (yes, no) as between-subject factor and *Privacy/Trust* as dependent variable, using the personal characteristic *Privacy Concerns* as covariate. We found a significant effect of privacy information on *Privacy/Trust* (p = .049). As expected, privacy information had a positive effect on attitudes regarding privacy and trust in the SWELL tool ($\mu_{control}$ = 3.85 vs. $\mu_{privacy}$ = 4.24, see Figure 4). Moreover, we performed an ANOVA with privacy information (yes, no) as between-subject factor and *Attitude towards Use* as dependent variable, using the personal characteristic *Motivation* as covariate. We did not find a significant effect of privacy information on *Attitude towards Use* (p = .616, $\mu_{control}$ = 4.03 vs. $\mu_{privacy}$ = 4.16). We also did not find a significant effect of privacy information on *Transparency* (p = .332, $\mu_{control}$ = 4.64 vs. $\mu_{privacy}$ = 4.86).

To further investigate the relationships between our 3 dependent variables we calculated Pearson correlations. We found a significant weak correlation between *Transparency* and *Privacy/ Trust* (r = .282, p = .001), meaning that a high score in transparency is slightly related to a high score in privacy and trust. We did neither find a meaningful correlation between *Transparency* and *Attitude towards Use* (r = .132, p = .143) nor between *Privacy/ Trust* and *Attitude towards Use* (r = .170, p = .059).

Summary. From our analyses we can conclude that attitudes regarding *Privacy and Trust* in the SWELL tool are moderately related to personal *Privacy Concerns*. Moreover, giving users privacy information seems to have a positive effect on perceived *Privacy and Trust* regarding the SWELL tool. We found that the *Attitude towards Use* of the SWELL tool is moderately related to personal *Motivation*, and contrary to our expectations, not related to attitudes on *Privacy and Trust*.

6 Discussion

Our first hypothesis was that when users have access to detailed information on data collection and privacy by design, they have less privacy concerns and more trust in the system. This hypothesis was confirmed in our user study. To build trust in your CAS it is a good idea to communicate information about data collection to the user and to address privacy.

Our second hypothesis was that users would have a more positive attitude towards using the CAS, as a consequence of trusting it more. This hypothesis was not supported by our data. We found that users base their attitude and intention to use the system mostly on the added value it has for them, and privacy and trust considerations might not be obvious or important enough to be taken into account. This has previously been found and termed the 'privacy paradox': people disclose personal information despite their privacy concerns [13]. We might see the consequences of this when users mindlessly accept all access rights in order to use a desired app. 'Privacy calculus' states that consumers weigh the risks against the benefits of disclosing information [6]. As far as users might be underestimating the risks, [3] suggests that responsibility for correct data usage should shift towards companies and away from users, who are often left in the dark after consenting to something they may not have read in full detail or understanding. Research has also shown that although people desire full control over their data, they favor technical and other supply-side solutions ('control paradox' [13]). Therefore we think it is important to implement privacy by design to adequately protect the privacy of the users.

We note that due to our methodology (using a presentation to outline the system and a questionnaire to assess the users' attitudes) only preliminary insights can be gained. Ideally, users should be asked to really install the CAS to do a more thorough analysis on the relation between perceived privacy and actual use of the system, which might deviate from stated attitudes and intentions, as pointed out by [6].

7 Conclusions

In this paper we addressed privacy and user trust in context aware systems (CAS), based on our SWELL use-case. As our SWELL system is a typical CAS in which context data is collected to provide the user with a service, the insights gained are also applicable to other CAS. In the first part of this paper, we found by means of a Privacy Impact Assessment the following important privacy aspects to address in CAS: *Goal of data collection, Type of data, Reactions to the system, User control, Quality* *of the data*, *Security of the data*, *Data responsibilities* and *Data sharing*.We outlined how these issues can be addressed from the developers side by presenting guidelines for Privacy by Design, which can be found in section 4.

In the second part of this paper we presented a user study, in which we found that privacy information had a positive effect on perceived privacy and trust in our system. We also found that the attitude towards using our system was related to personal motivation, and not related to perceived privacy and trust. Therefore we think it is important to implement privacy by design to adequately protect the privacy of the users in context aware systems.

Acknowledgements. This publication was supported by the Dutch national program COMMIT (project P7 SWELL).

8 References

1. Dey, A. K., Brown, & Abowd, G. D. (1999). Towards a better understanding of context and context-awareness. In *Handheld and ubiquitous computing* (pp. 304-307). Springer Berlin Heidelberg.
2. Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review, 26*(1), 20-43.
3. Rubinstein, I. (2012). Big Data: The End of Privacy or a New Beginning?. *NYU School of Law, Public Law Research Paper,* (12-56).
4. Jiang, X., Hong, J. I., & Landay, J. A. (2002). Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *Ubicomp 2002: ubiquitous computing (pp. 176-193).* Springer Berlin Heidelberg.
5. Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5).
6. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly, 35(4),* 989-1016.
7. Barkhuus, L., & Dey, A. K. (2003). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In *INTERACT (Vol. 3,* pp. 702-712).
8. Koldijk, S. (2012). Automatic recognition of context and stress to support knowledge workers. In: *Proceedings of ECCE 2012* (Edinburgh, Scotland, 28-31 August 2012).
9. Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review, 28(1),* 54-61.
10. Cavoukian, A. (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices.* Ontario: Information and Privacy Commissioner of Ontario.
11. Hoepman, J. H. (2012). Privacy Design Strategies. *arXiv preprint arXiv:1210.6621*.
12. Bodea, G., Huijboom, N., Kazemier, J., Koldijk, S., Koot, G., de Munck, S. & Siljee, J. (2013). *Context-aware services: privacy concerns and strategies*. TNO report.
13. Compañó, R., & Lusoli, W. (2010). The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. In *Economics of Information Security and Privacy* (pp. 169-185). Springer US.