Privacy by Design Principles in Design of New Generation Cognitive Assistive Technologies

Ella Kolkowska, Annica Kristofferson

Privacy by design principles in design of new generation cognitive assistive technologies

Ella Kolkowska[1], Annica Kristofferson[2]

[1] Örebro University School of Business, Sweden
[2] School of Science and Technology, Örebro University, Sweden
{ella.kolkowska, annica.kristoffersson}@oru.se

Abstract. Today, simple analogue assistive technologies are transformed into complex and sophisticated sensor networks. This raises many new privacy issues that need to be considered. In this paper, we investigate how this new generation of assistive technology incorporates Privacy by Design (PbD) principles. The research is conducted as a case study where we use PbD principles as an analytical lens to investigate the design of the new generation of digitalized assistive technology as well as the users' privacy preferences that arise in use of this technology in real homes. Based on the findings from the case study, we present guidelines for building in privacy in new generations of assistive technologies and in this way protect the privacy of the people using these technologies.

Keywords: Privacy requirements, Privacy by Design, assistive technology, cognitive decline, aging in place

1 Introduction

Assistive technology (AT) is a broad term used to describe any item, object, device or system that enables disabled people to perform a task that they would otherwise be unable to do, or increase the ease and safety by which certain tasks can be performed. AT plays an important role in supporting elderly people in living independently at home [1]. In this paper, we focus on AT suitable for elderly with a mild cognitive decline, e.g., dementia. The rapid development of cognitive assistive technologies (CAT) paves the way for new and more efficient solutions that improve the quality of life for people being affected by cognitive decline while decreasing their caregivers' burden of care [2]. Today, we are rapidly moving from analogue CAT accessible only for the user of the specific device to digital replicas, and further extensions of the CAT involving sensor networks but also technologies accessible by remote caretakers. In this paper, we refer to this technology as *the new generation of CAT*. The development of CAT raises many new privacy issues which need to be considered [3-5] but unfortunately, most of today's development projects are technically oriented and focus on functionality and technical effectiveness of the developed solutions [5, 6]. Consequently, the privacy of the user is often not sufficiently considered during development and implementation of the new generation of CAT [5].

The concept of *Privacy-by-Design (PbD)* advocated by EU [7] aims to ensure privacy protection and personal control over the information collected when IT systems are used. PbD principles are formulated to support the designers in taking the protection of privacy into account during the development of technologies (such as CAT) that in turn results in better privacy protection for the users of these technologies.

In this paper, we investigate how the *new generation of CAT* incorporates PbD principles with respect of elderly users' privacy requirements. Based on our findings, we formulate a set of guidelines for building in elderly users' privacy preferences into CAT and in this way protect the privacy of the people using them. A starting point for this research is a set of PbD principles suggested by Cavoukian et al. [8] for the context of personal health monitoring. The main contribution of the paper is adding a users' perspective to the existing technology-focused PbD principles.

The paper is structured as follows. Section 2 describes and discusses the PbD concept and PbD principles. Section 3 describes the new generation of CAT at focus in this case study. Section 4 presents our research method. Section 5 reports on our analysis of the case study. In section 6, we discuss the results and present a set of guidelines for building into privacy in the new generation of CAT. Section 7 concludes the paper.

2 Privacy by Design principles

Protection of privacy regarding sensitive personal data, is legally regulated in most countries and therefore cannot be overlooked in design and use of the new generation of CAT. It is also recognized that people, generally are not capable or not interested in protecting their own sensitive information, thus there is a need for standardization and automatization of privacy protection [7]. PbD is a way of embedding privacy into the design specifications of technologies. Cavoukian et al [8] suggest seven PbD principles for the context of personal health monitoring These seven principles are an adjustment of the general OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" [8]. The seven PbD principles formulated by Cavoukian et al. for the context of health care monitoring are [8]:

1. Proactive not Reactive; Preventative not Remedial. The PbD approach is characterized by proactive rather than reactive measures. The first principle emphasizes that it anticipates and prevents privacy invasive events before they happen.

2. Privacy as the Default Setting. The second principle means that no action is required by the users to protect their privacy because it is built into the system, by default.

3. Privacy Embedded into Design. The third principle emphasizes the importance of embedding privacy into the design and architecture of IT systems and business practices from the beginning and not add it afterwards.

4. Full Functionality - Positive-Sum, not Zero-Sum. The fourth principle considers privacy as an integral part of the system without diminishing its functionality.

5. End-to-End Security - Full Lifecycle Protection. The fifth principle relates to the life cycle management of information and stresses that data should be protected in all data handling from its beginning (collection) to its end (destruction). I.e., this principle is important to ensure privacy of the people using the technology when it is in use.

6. Visibility and Transparency - Keep it Open. The sixth principle states that data protection should be visible and transparent to the different stakeholders, e.g. users and providers. In the context of our case study, this principle means that the users are informed about what data is being collected and for what purpose, how the data is being used, and who can access it.

7. Respect for User Privacy - Keep it User-Centric. This principle means that the individual's privacy should be an interest of designers and operators of health systems.

Cavoukian et al. [8] define information privacy as an individual's ability to exercise control over the collection, use, disclosure and retention of his or her personal information, including personal health information. Nordgren [9] argues that the PbD principles suggested by Cavoukian et al. are supportive in ensuring privacy of the patients in the context of personal health monitoring, although they have two limitations: 1) PbD cannot solve all privacy problems because responsible handling of information by human agents is also important, and 2) automated data protection is useful in many cases, but it is not desirable in all cases. Generally, socially-oriented research on privacy in this context is sparse. Previous research shows that elderly people's privacy preferences are not sufficiently investigated in development of CAT [5, 10, 11]. Usually, it is assumed-at least implicitly-that a "common" CAT user does not care about privacy [11]. Consequently, development of such technologies is often functionality-driven without taking care of privacy issues that arise in use of such technologies in real settings [5, 6]. That is against the PbD thinking. Our interest lies in studying the privacy concerns that arise in use of CAT in real settings as well as their potential, in case of unforeseen usage in the future. Since the importance of respecting the users' privacy is especially empathized in the seventh PbD principle we decided to conduct a case study focusing on the users' privacy preferences that come up in use of CAT in relation to Cavoukian et al.'s seven PbD principles.

3 System description

An example of the new generation of CAT is HOMEbasic[1], which is a "safety and security" package for those who need a combination of time and memory support, environmental monitoring and alarm functionalities. HOMEbasic in its standard package consists of a MEMOplanner and a sensor network (a door magnet, a stove sensor, an on/off sensor, two motion sensors and a lamp actuator). The MEMOplanner supports the user with the calendar reminders and sensor-based reminders listed in Table 1 by issuing an auditory and visual reminder. Additionally, the light is automatically turned on when the user's feet are detected beside the bed to minimize the risk of falls during nighttime. In the current version, all information is saved locally within the MEMOplanner. While disabled by default upon delivery, a USB remote control can be provided to those who need to administer MEMOplanner. Provided that MEMOplanner is connected to the Internet, users (for example relatives or caregivers) with the USB can access all functionalities in MEMOplanner, i.e. also Windows. There is only one

[1] Abilia, HOMEbasic i2, http://www.abilia.com/sv/produkt/homebasic-i2?product_category=34 2015-11-09

access level for remote administrators, hence, users provided with a USB can access and edit the content of the calendar, contacts, and photos from remote. A Vera 3 gateway communicates both with the sensors using the Z-wave protocol[2] and with the MEMOplanner (usually via WiFi but a cabled connection is possible). The Vera gateway can also connect the MEMOplanner to the Internet. By default, the triggered reminders are not stored within the Vera or sent remotely to any administrator.

Table 1. Summary of functionality of HOMEbasic

1.	*Calendar visualisation*: Information of time. Calendar for structuring daily tasks. The user (or a remote user) can add new events to the calendar. Each event can consist of sub events. It is also possible to add the relative's daily activities helping the person with memory decline keep track of his/her relatives' activities
2.	*Calendar reminders:* Reminders about upcoming events.
3.	*Additional functionality:*Skype, photo album, contacts
4.	*Sensor-based reminders:* Stove on but no motion in kitchen for x minutes. An electronic device has been turned on for x minutes. The entrance door is opened while the stove is on. The entrance door is opened. Can be used to remind the user to, e.g., lock the door or to tell the user that it is not an appropriate time to go out.
5.	*Sensor-based actuation:* Lamp automatically turned on when motion beside bed.

4 Research method

This research was conducted as a case study where we investigated the CAT described in Section 3, as well as privacy concerns that arose in use of this technology in real homes. Although results from case study research cannot be statistically generalized, this approach supports collection of rich context-specific details and in this way reveals important information about the object under study and increases the understanding of the specific context [12]. By using this methodology, we were able to study the users' expectations and needs regarding privacy and the new generation of CAT's possibility to address these needs in depth.

4.1 Selection of participants

We looked for test persons who had some sort of a cognitive decline. All seven test persons (μ = 71.6 years old) were men and lived together with their wives (μ = 65.7 years old) in ordinary housing/private residences outside nursing homes. All test persons and four of the wives were retired. Two wives were still working full-time and one was working part-time. Additional details about the case settings can be found in [13].

[2] Abilia, MEMOplanner Handbook, fttp://www.abilia.com/sites/abilia.com/ files/field_resource_file/4X2650_Handbook_MEMOplanner_S525.pdf 2015-11-06

In sum, the CAT was deployed and used in seven Swedish homes during a period of approx. six months.

4.2 Data collection

Data was collected in five stages: 1) functionality and privacy in design of HOMEbasic, 2) users' general privacy preferences, 3) observation of users' privacy preferences when using HOMEbasic, 4) users' privacy preferences in relation to HOMEbasic's current and future functionality (scenarios), and 5) users' opinions about the methods used for implementation and introduction of HOMEbasic.

Stage 1: functionality and privacy in design of HOMEbasic. In this stage, we wanted to gain a general understanding about HOMEbasic's functionality and the implemented privacy measures. For that reason, we participated in two demonstrations of HOMEbasic where we could interact with the system and ask questions. We also reviewed the HOMEbasic documentation and manuals and interviewed the developers. Finally, we interviewed experts responsible for prescription of this (and similar) CAT to end-users.

Stage 2: users' general privacy preferences. In this stage, data was collected through semi-structured interviews with the test persons and their relatives when the CAT was deployed. The interviews aimed to collect data about the participants' general requirements and preferences regarding privacy and their expectations/worries regarding privacy of information handled by the CAT. At this first interview session, the test persons and their relatives were interviewed separately. The interviews focused on three areas: 1) general privacy awareness and preferences, 2) privacy preferences in interaction with health care and elderly care, 3) privacy concerns in relation to use of the CAT. Aspects discussed within these areas were related to: the interviewees' privacy enhancing behaviors when using ICT, knowledge about privacy regulation, privacy awareness, privacy concerns etc.

Stage 3: observation of users' privacy preferences when using HOMEbasic's. During the test period, we visited the test sites regularly and observed how the CAT was used. We also discussed users' privacy concerns that come up during the use of CAT.

Stage 4: users' privacy preferences in relation to HOMEbasic's current and future functionality. This stage focused on privacy concerns in relation to present and future potential functionality of the CAT and was conducted when the CAT was removed from the homes. Future scenarios were developed based on the current trends in development of CATs aiming at integrating these technologies as a part of health care and home care. For that reason, it is assumed in some scenarios that health care professionals and home care staff are able to access the data collected by the CAT. Use case-based scenarios steered the interview. We formulated at least one scenario for each CAT existing functionality in the CAT (see Table 2) and several possible scenarios for use of this functionality in the future. By default, the triggered alarms are not stored within the Vera or sent remotely to any administrator. However, accessing information about trigged alarms could allow home care staff and/or health care professionals to monitor changes in behaviors of the person using a CAT. For instance, more frequent actuation of the lamp sensor at nights could indicate that the elderly person has sleep problems or more frequently issued sensor-based reminders could indicate a decline of the elderly

person's health condition. Such information could help the caregivers to react on the changes and help the elderly person in a more efficient way. Thus we included scenarios 10-15 assuming that it will be possible in the future.

For each scenario, the participants were asked a few questions revealing their privacy preferences, for instance: How does it make you feel? Why? What emotions does this event raise? Why? How would you like to change the situation to feel okay?

Table 2. CAT's functionality and scenarios used during the interviews

Calendar visualisation.
Scenario 1: How would you feel if someone from your family or acquaintances studied the MEMOplanner with your daily tasks planned in it?
Scenario 2: Would you feel differently if it was a stranger e.g., someone helping with the renovation, who looked at your planned tasks? For instance, if you had planned a holiday?
Remote access (future scenarios)
Scenario 3: In this stage the test person gets help from home care staff and they can remotely access Memoplanner. A number of activities for both the test person and the relative are added in the MEMOplanner The test person is contacted by home care staff, pointing out that he exercises too little.
Scenario 4: The relatives is contacted by home care staff pointing out that she should encourage her husband to exercise more.
Calendar reminders.
Scenario 5: You have a party and there are a number of people in your home, acquaintances and family. The calendar reminds that [name of the test person] needs to take his medicine. The guests look at the calendar, some of them ask what it is. Some ask how [the test person] feels.
Scenario 6: Would you feel differently if it was a stranger, e.g., someone helping with the renovation who heard the reminder?
Additional functionality (future scenarios)
Scenario 7: You use the possibility to store photos in the MEMOplanner, i.e., you keep private photos of your family, photos from your vacation etc. After you come back from the holiday, home care staff comment on your holiday's photos which you have not shown them.
Scenario 8: Would you feel differently if they commented on pictures of your grandchildren from the last party?
Scenario 9: After a while you discover that your private pictures are used in an advertisement of the hotel on the Internet.
Sensor-based reminders (future scenarios)
Scenario 10: The stove sensor is installed and you feel that it fulfils its goal and runs the reminders when needed. On the next visit, your doctor tells you that your memory has declined because she/he can see that the reminders from the stove sensor runs more frequently.
Scenario 11: Would you feel differently if you knew that the doctor is able to see this information?

Scenario 12: Would you feel differently if it was a home care personnel who told you about the memory decline?

Scenario 13: The doctor points out that [the relative] should take more responsibility for cooking.

Sensor-based actuation (future scenarios)

Scenario 14: The motion sensor is installed in the bedroom. You feel that it works well and it feels safe when the lamp automatically turns on when you go up at night. You are contacted by the home care personnel who ask if you need any help with sleeping since they noticed that you go up often at nights.

Scenario 15: On the next visit, the doctor ask why you go up so often at nights. He/she suggests a medicine to help you sleep better.

Stage 5 users' opinions about the methods used for implementation and introduction of HOMEbasic. This interview session, which was conducted one month after the CAT had been removed, focused on the test person's and the relative's reflections on the approach taken in this case study. The questions asked during these interviews were: What do you think about the information you got about the CAT? What do you think about the introduction and training? In relation to each question, we asked several follow up question such as: Was it enough/not enough? How would you like to get the information/training? What was missing?

4.3 Data analysis

The collected data was analyzed in 4 steps. First, we identified the privacy preferences highlighted by the users in relation to the CAT's functionality during all stages of data collection. Second, we identified the privacy implementations from the material collected during the first stage of data collection in order to find how PbD principles were incorporated into the design of HOMEbasic. Third, we identified the users' unsolved privacy requirements in relation to each of these principles. Finally, based on the analysis and current literature, we formulated guidelines for applying PbD principles in design of the new generations of CAT.

5 CAT users' privacy requirements

In this section we describe users' privacy requirements in relation to the current and possible, future functionality of HOMEbasic. The section is structured according to the functionality categories presented in Table 1. For clarity, illustrative examples in relation to each principle are provided.

5.1 Calendar visualization

Some privacy concerns regarding this functionality came up already during the second stage of data collection (see Section 4.2), when we asked about users' privacy concerns in relation to HOMEbasic before they started to use it. Mainly the relatives expressed

privacy concerns in this stage, while the test persons were less worried about privacy violation when using HOMEbasic. For instance, a relative in the test site that still had a teenage child at home was very concerned about the child's privacy and did not want to add any events that would reveal information about the child into the calendar even if this information would be helpful for the father who suffered from a strong cognitive decline. Another wish that came up during this stage of data collection was the possibility to delete "old" data stored in the MEMOplanner. This requirement was expressed by both the test persons and their relatives. Users preferred the data to be deleted frequently by default but if it was not possible they wanted to be reminded to do it by themselves. The users informed that the MEMOplanner may store detailed descriptions about how the activities should be performed, including sensitive information about the test person's health condition and needs. An interesting reflection that was made by one of the relatives during this stage of data collection was that privacy requirements change in line with progression of the disorder. The respondent explained: *I think that when you get to that stage when you can no longer cope with things alone and need home care to help you with everything, the privacy is already forgotten. It is a sad part of it, but so it is.* This means that privacy requirements are not static and that the new generation of CAT should be able to handle these changes.

During this stage of data collection, two relatives also mentioned a need for limiting access to the information visible in the MEMOplanner. This need becomes more apparent during stage 3 and 4 of the data collection. For instance during stage 3, we could observe that one of the wives kept deleting events that already occurred from the calendar. Asking her about the reason for doing it, she answered: *We could have done something in the morning, then maybe we had guests in the afternoon or evening, and then I thought that they did not need to know what we have done in the morning.*

When discussing scenarios 1-2 in stage 4 of the data collection, we found that both the test persons and the relatives are concerned about possible privacy violations when the information in the MEMOplanner is visible for strangers who for different reasons are present in the elderly peoples' home. One of our respondents told us: *I would not like it if a stranger looked at our planning [in the MEMOplanner]. I would feel uncomfortable. In this case, I would need to turn the calendar off, or somehow make information invisible. For now, the calendar is completely open.* Another respondent explained: *The idea is to put everything in the MEMOplanner, e.g., that you have to visit a special doctor. You may not want everyone to know about this and about what you do during the days. I think it depends on family relationships and how you are as a person. Some people do not want others to know anything…*. Thus, we identified a clear need for a possibility to sometimes hide the information in the MEMOplanner.

5.2 Calendar reminders

The users' privacy concerns related to this functionality were identified mainly in stage 3 and 4 of the data collection (see Section 4.2). For instance, while visiting a test site, we noticed that the volume of the reminders was heavily lowered. As a consequence, the test person could hardly hear the voice reminders. When we asked them why they lowered the volume for the reminders, the wife explained that she felt embarrassed

when the neighbors could hear the voice reminders so she decided to lower the volume. Additional clear privacy preferences were formulated by the users during stage 4 when we discussed scenarios 5 and 6. We found that the users had different privacy preferences regarding this functionality. While some users did not mind if other people heared the reminders, other users were clearly uncomfortable with this. One of our test persons told us: *I don't feel comfortable with this. It makes you feel sick! I try not to think about my disorder all the time. In this case, I would get lots of questions that I do not want to get or discuss. It's a party and I also want to have fun. I would like the MEMOplanner or the reminders to be switched off just then.*

5.3 Additional functionality and remote access

Privacy concerns related to this, future possible way of using MEMOplanner were revealed during stage 4 when we discussed scenarios 3-4 and 7-9. The current version of the MEMOplanner offers the possibility to store contacts and photos and to use Skype for communication. In the future scenarios, we assumed that home care personnel will have remote access to the MEMOplanner to be able to help the user to plan the activities. In the current version of the CAT, all information is equally accessible for all users and there is no possibility to restrict access to certain parts of the stored data. However, while discussing scenarios 3-4 and 7-9, we found that photos and in some cases contacts are considered as sensitive for some users and for that reason they should not be accessible for all categories of current or future users. One test person told us: *I would not like it if the homecare staff looked at my photos without permission. This is not a part of their job! Maybe they would not do it, but because I cannot prevent it, I cannot be sure.* Thus, the users emphasized the importance of access control mechanisms allowing them to decide who is permitted to access specific information stored in the MEMOplanner (e.g., planning, details regarding each planned event, photos etc). One of the users said: *you do not want everyone to know what information you put in [the calendar]. Then you can get worried about how that information is disseminated. You should be able to control who sees what. As it is in other systems; some people can access the information and others cannot.*

5.4 Sensor-based reminders and actuation

Privacy concerns in relation to the future use of these functionalities were discussed in stage 4 of the data collection using scenarios 10-15. We found that most test persons would welcome such functionality if the main reason for it was to help them in their disorder. However, there was a clear difference in the users' privacy concerns depending on which group of caregivers that would monitor the sensor-based reminders and actuations. The users did not have any restrictions in the case of health care professionals. They did not even care if they would be informed about the monitoring in advance or not. The users were more restrictive in the case of homecare staff. They could accept the monitoring if they were informed in advance about the purpose and extent of the monitoring. They also highlighted it as important to limit the number of home care staff (preferably only one contact person) that could access the log data. Generally, they felt

that monitoring could increase their sense of safety at home, when they could no longer cope with the basic things by themselves.

Table 3 summarizes the users' privacy requirements (R) in relation to CAT's functionality. Some of the requirements were clearly stated by the users, others were derived by the researchers based on users' statements.

Table 3. Summary of the users' privacy requirnements in relation to CAT's functionality

Calendar visualisation.
R 1: a possibility to delete "old" data stored in the CAT (by default)
R 2: new generation of CAT needs to handle changes of users' privacy needs
R 3: a need for a possibility to sometimes hide the information visible in the CAT
Calendar reminders.
R 4: a need for a possibility to sometimes switch off voice reminders
Additional functionality and remote control
R5: a need for access control mechanisms allowing the users to decide who is permitted to access specific information stored in the MEMOplanner
Sensor-based reminders and actualisations
R 6: a need to differentiate the access to the collected sensor data dependently of the caregivers
R7: a need for knowing in advance about the purpose and extent of the monitoring.
R 8: a need to limit the number of home care staff (preferably only one contact person) that could access the log data

6 Guidelines for applying PbD principles in design of CAT

In this section, we discuss findings from the case study in relation to the PbD principles formulated by Cavoukian et al. [8] and existing literature. Based on the discussion, we formulate a set of guidelines for applying PbD principles in design and use of the new generation of CAT.

6.1 Principle 1: Proactive not reactive; Preventative not remedial

The importance of privacy protection is not emphasized in the documentation of the CAT which focuses on the description of functionality allowing users to live safely and independently in their homes. Based on the documentation, we can conclude that the design of HOMEbasic is safety- and functionality-driven and users' privacy is not especially emphasized. However the users highlighted many privacy concerns in relation to the existing and future possible use of CAT (see Section 5). They also expressed several privacy requirements in relation to this technology (see Table 3). Following the first PbD principle means to design CATs with these privacy requirements in mind to be able to prevent privacy invasive events before they happen. Therefore the identified privacy requirements should be considered when CAT are designed. Another important finding from our case study is that different users experience different events as privacy

invasive and that contexts in which CAT are used are very different. The problem of not addressing the diversity of elderly users is highlighted in literature. The elderly users are often treated as a homogenous group with similar needs and preferences [5, 11]. But to be able to truly meet elderly peoples' needs and preferences, the designers need to acknowledge and understand the differences [6]. *Thus, the designers of the new generation of CAT should consider the variety of users and contexts in which CAT can be used and design adaptable privacy solutions that prevent the privacy invasive events to happen (Guideline 1)*. By adaptable solutions we mean flexible solutions that are possible to adapt to the diverse privacy requirements and diverse context of the elderly users homes.

6.2 Principle 2: Privacy as the default

We found that privacy is built into HOMEbasic to some degree. For instance, the product's documentation states that the possibility to remotely access the MEMOplanner is disabled by default and must be turned on manually because of privacy concerns. In this way, the data stored in the MEMOplanner is protected against unauthorized usage by default and the users do not need to take any additional action to protect the sensitive data in the default setup.

However, we discovered several examples (see Section 5) when protection of privacy required users to actively take necessary actions, otherwise there was a risk for privacy violation. In some cases, the desired level of protection was not even achievable because of lacking technical implementations, i.e., access control and screen saver. We found that our participants would like the CAT to protect their privacy by default. Protecting privacy by default may result in inflexible and unadaptable solutions that cannot handle changing privacy requirements. As described in Section 5.1, the elderly person's health situation can change over time and this can lead to changed privacy preferences. Treating privacy requirements as static is considered as being problematic in the literature [5, 14]. *Thus, the designers of the new generation of CAT should investigate users' privacy preferences to find situations when privacy protection can be built into the technology by default. Default settings should be balanced with flexibility (Guideline 2)*

6.3 Principle 3: Privacy embedded into design

Regarding the third principle, we found that users would like to have additional technical solution to protect their privacy. It is argued in literature that most people are not capable of protecting their own sensitive information [9], thus embedding privacy in technical solutions is important. However it is also argued that solely technical solutions cannot solve the complex privacy challenges that arise when using the new generation of CAT [5]. *Thus, designers of new generation of CAT should provide users with privacy guidelines and recommendations on how to protect privacy when the CAT is in use. Such guidance is missing in the CAT's documentation and manuals. (Guideline 3)*

6.4 Principle 4: Functionality—Positive-sum, not zero-sum

Our findings in relation to principle 4 indicate that it is not easy to balance utility and privacy in use of the new generation of CAT. In the provided examples (see Section 5), we can see that privacy measures such as hiding information in the MEMOplanner or lowering the volume of the reminders may lead to a decreased possibility to support the person affected by cognitive decline (see Section 5.1 and 5.2). The conflict between privacy and other values such as safety and autonomy is well known in literature and often highlighted as problematic [9]. *Thus, designers of the new generation of CAT should perform a privacy and utility analysis when a new functionality is added to the system (Guideline 4). There are situations where new functionality does not contribute to utility and jeopardize privacy*. Such development should be avoided.

6.5 Principle 5: End-to-end lifecycle protection

Although we studied only a small sample of seven test sites, we could observe differences in privacy preferences that depended on contextual variables such as family situation, family relationships, how active the elderly people were and how many people who visited their homes. We argue that these different privacy needs would not be identified if we did not studied the use of CAT in real settings. Thus, we can conclude that it is important to study CAT in use to be able to implement privacy measures that are relevant and adapted to the specific needs of the different users. The problem of a lack of real experiences of using CAT in practice and thus a lack of knowledge about possible privacy concerns that can arise when using such technology is highlighted in literature as problematic [3, 11]. *We argue that designers of CAT should consider privacy aspects regarding the use of CAT in real settings already during the development process (Guideline 5)*. It can be done by involving significant stakeholders, such as primary users, secondary users, health care professionals, and other formal and informal caregivers in design of CAT.

6.6 Principle 6: Visibility and transparency

To comply with this PbD principle is a challenge in the CAT context because often elderly people have difficulties in understanding the consequences that the implemented technology have on their privacy. The problem is also highlighted in literature. For instance Bowes at al. [11] argue that elderly people do not have the necessary (technical) background to formulate the appropriate privacy requirements and understand the privacy consequences of the implemented CAT. Although most of the participants told us (see 4.2, stage 5) that they experienced the CAT to be complex and sometimes difficult to use, they were able to discuss privacy issues in relation to it. The understanding came after they had used the CAT for some time in their homes and because we used methods and tolls to exemplify and visualize current and future use of the CAT i.e. scenarios, audio/video presentation .*Thus we argue that it is important to use specific methods and tools to make the privacy consequences understandable and clear for the elderly people who will use the new generation of CAT (Guideline 6).*

6.7 Principle 7: Respect for the users' privacy

Regarding the seventh principle, we can conclude that elderly people are both capable and willing to engage in discussions about their privacy preferences. We also found (see Section 4.2, stage 2) that elderly people do care about privacy. Generally, they are careful about how they reveal their personal information in use of technology, Internet, social media and even in their everyday life. They are mostly concerned that their personal information may be used by criminals. Regarding revealing health information, they totally trust health care professionals and are not concerned about providing such information to health care organizations. Regarding privacy in relation to information handled by CAT, we can conclude that the preferences differed between the users' depending on personal preferences, environmental factors, and family relationships. *Thus, we argue that designers of CAT should involve the elderly users in the design of the new generation of CAT and the design of privacy solutions in relation to this technology (Guideline 7).*

7 Conclusion

The rapid development of cognitive assistive technologies (CAT) from simple analogue assistive devices into complex and sophisticated sensor networks raises many new privacy issues that are not sufficiently addressed in design and use of these technologies in real homes. This paper investigated how the new generation of CAT incorporates PbD principles suggested by Cavoukian et al. [8]. Special attention was put on that users' privacy preferences that arise in use of new generation of CAT in real homes. Based on our empirical findings and a literature review, we suggest a set of guidelines for applying Cavoukian et al.'s PbD principles in design and use of the new generation of CAT. Using these guidelines will help to build in users' privacy requirements in the design of a new generation of CAT and in this way protect the privacy of the elderly people using these technologies.

Generally, we can conclude that the existing PbD principles focus on technical aspects of privacy and often reduce privacy to the protection of personal data. Our examples (see section 5) show that some privacy concerns arising in the use of CAT are beyond this narrow view of privacy. For instance, we found that privacy in this context is not only related to the primary user of the CAT but also to people who are in the user's environment such as a child or wife etc. We argue that more research of non-technical privacy aspects of privacy in this context is needed.

Acknowledgment. The authors would like to thank the elderly participants and the Länsförsäkringar Research Foundation for making this study possible.

References

1. Frennert, S.A., Forsberg, A., Östlund, B.: Elderly People's Perception of a Telehealthcare System: Relative Advantage, Compatibility, Complexity and Observability. Journal of Technology in Human Services 31, 218--237 (2013)

2. Koch, S., Marschollek, M., Wolf, K.H., Plischke, M., Haux, R.: On health-enabling and ambient-assistive technologies. What has been achieved and where do we have to go? . Methods of Information in Medicine 48, 29--37 (2009)
3. Kosta, E., Pitkänen, O., Niemelä, M., Kaasinen, E.: Mobile-centric ambient intelligence in Health- and Homecare-anticipating ethical and legal challenge. Science and Engineering Ethics 16, 303--323 (2010)
4. Shankar, K., Camp, L.J., Connelly, K., Huber, L.: Aging, Privacy, and Home-Based Computing: Developing a Design Framework. Pervasive Computing october-december, 46--54 (2012)
5. Zwijsen, S.A., Niemeijer, A.R., Hertogh, C.M.P.M.: Ethics of using assistive technology in the care for community-dwelling elderly people: An overview of the literature. Aging & Mental Health 15, 419--427 (2011)
6. Frennert, S.A., Östlund, B.: Review: Seven Matters of Concern of Social Robots and Older People. International Journal of Social Robotics 6, 299--310 (2014)
7. European Commission: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2012)
8. Cavoukian, A., Fisher, A., Killen, S., Hoffman, D.: Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design. Identity in the Information Society 3, 363--378 (2010)
9. Nordgren, A.: Privacy by Design in Personal Health Monitoring. Health Care Analysis 23, 148--164 (2013)
10. Mort, M., Roberts, C., Pols, J., Domenech, M., Moser, I.: Ethical implications of home telecare for older people: a framework derived from a multisited participative study. Health Expectations 18, 438--449 (2015)
11. Bowes, A., Dawson, A., Bell, D.: Implications of Lifestyle Monitoring Data in Ageing Research. Information, Communication & Society 15, 5--22 (2012)
12. Yin, R.K.: Case Study Research-Design and Methods. Thousand Oaks: SAGE Publications, USA (1994)
13. Kristoffersson, A., Kolkowska, E., Loutfi, A.: Assessment of Expectations and Needs of a Sensor Network to Promote Elderly's Sense of Safety and Security. In: the Seventh International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, CENTRIC 2014, pp. 22--28 (2014)
14. Remmers, H.: Environments for ageing, assistive technology and self-determination: ethical perspectives. Informatics for Health & Social Care 35, 200--210 (2010)