Privacy Principles in Design of Smart Homes Systems in Elderly Care

Ella Kolkowska(✉)

Örebro University School of Business, Örebro, Sweden
ella.kolkowska@oru.se

Abstract. Privacy is considered as a main concern in developing and implementing smart home systems for elderly care (SHSEC). Privacy-by-Design (PbD) can help to ensure privacy in such systems and can support the designers in taking the protection of the privacy into account during the development of such systems. In this paper, we investigate the suitability of the PbD principles (PbDPs) suggested by Cavoukian et al. [1] in the context of SHSEC. This research is conducted as a qualitative case study, where we highlight limitations of existing PbDPs in this context. Based on our findings, we suggest seven additional PbDPs which complement the existing PbDPs and adjust them in the context of SHSEC.

Keywords: Privacy by design · Aging in place · Smart home system · Privacy · Elderly

1 Introduction

A smart home network is a unified combination of people, wireless networks, and other technical devices [2]. By using this technology, a smart home system (SHS) can provide information about activities and the status of different entities in the home environment. Recently, smart home technology has been used to support the independent living of elderly people allowing them to stay at home as long as possible [3, 4]. Using smart home technologies in elderly care is beneficial in many ways. The elderly can live longer independently in their homes where they usually have a richer social life and can maintain established habits. For caregivers, such solutions reduce their workload and for the society, smart home solutions substantially decrease the costs for elderly care since the cost of care at home is almost always a fraction of the cost of residential care [5]. However, to allow the elderly to stay at home, the smart home technologies must ensure the safety of the residents and give caregivers the opportunity to quickly react to any health problem or any emergency in the smart home. This is realized by extended monitoring of the activities of the inhabitants [6], which raise many new privacy concerns [3, 7]. Ensuring privacy of the elderly is thus one of the main concerns in design of smart home systems in elderly care (SHSEC). This is one of the reasons why the EU advocates the principle of privacy-by-design (PbD) [8].

However there are different ways in how PbD is understood and applied in practice because of the different needs and the differences in defining privacy in various contexts

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 526–537, 2015.
DOI: 10.1007/978-3-319-20376-8_47

[3, 9]. Kosta et al. [10] argue that applying general ethical guidelines in the context of SHSEC is difficult because of the complexity of this environment and because of the conflicting interests that can arise between the different stakeholders within such environment. It is also recognized that ethical issues such as privacy that can come up in relation to the development and implementation of SHSEC are not sufficiently focused during the development of such systems [11]. Most of today's projects are technically oriented and focus on development and effectiveness of these technologies [7, 12]. Thus development of practical privacy guidelines that can be easily adapted in this context is seen as a real challenge [10]. The aim of this paper is to highlight limitations of existing PbDPs in the context of SHSEC and suggest a set of PbDPs adjusted to this context. A starting point for this research is a set of PbDPs suggested by Cavoukian et al. [1] for the context of personal health monitoring.

The paper is structured as follows. Section 2 contains a discussion about privacy in the context of SHSEC. In Sect. 3 we present our research method. Section 4 reports on our analysis of the case study. In Sect. 5 we present a set of PbDPs applied in this context. Finally the paper ends with conclusions in Sect. 6.

2 Privacy in the Context of SHSEC

New technologies such as SHSs are promoted as a means of retaining autonomy and quality of life for elderly people enabling them to continue to live independently in familiar settings [11]. The decreasing costs of such technologies together with their increased efficiency and portability create almost limitless possibilities to collect, process and communicate physiological and environmental data from the smart home to different stakeholders such as relatives, health care personnel, social workers etc. [13]. The complexity and special characteristics of SHSEC environments raise new privacy issues that are very different from those related to traditional applications and systems [3, 10].

Some scholars [i.e. 14] argue that the elderly people themselves do not worry about privacy and do not experience the monitoring devices in their homes as something disturbing. However, other studies [i.e. 3] show that privacy concerns are one of the biggest barriers to the successful implementation of SHSECs in practice. Nordgren [9] argues that some individuals are concerned about their privacy and some are not, but because we do not know it in advance, privacy has to be protected for everyone [9]. Moreover ensuring privacy of sensitive personal data, such as monitoring data, is regulated by law in most of the countries and therefore, it cannot be ignored. It is also known that most of the people are not capable of protecting their own sensitive information and thus the privacy protection has to be standardized and automatized by PbD [8]. According to Cavoukian et al. [1], PbD is a concept of embedding privacy into the design specifications of technologies. The authors suggest seven PbDPs for the context of personal health monitoring: (1) Proactive, not reactive; preventative, not remedial, (2) Privacy as the default, (3) Privacy embedded into the design, (4) Functionality —positive-sum, not zero-sum, (5) End-to-end lifecycle protection, (6) Visibility and transparency, and (7) Respect for users' privacy. These principles are an adjustment of general OECD

"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". Nordgren [9] discuss the suitability of the PbDPs suggested by Cavoukian et al. [1] in ensuring privacy of the patients in the context of personal health monitoring and concludes that the principles are supportive in ensuring privacy of the patients in this context. In this paper we study the suitability of these principles in the context of SHSEC.

3 Research Method

This study was conducted in the context of the European project GiraffPlus (http://www.giraffplus.eu/). GiraffPlus aims at developing a SHS that supports independent living for the elderly who wish to remain in their homes as long as possible. GiraffPlus is a complex system of sensors and a telepresence robot, Giraff, which is used for both monitoring and communication. In this project, special emphasis is put on evaluations and on feedback from both the primary and secondary users. Primary users are the elderly people who will actually be using the GiraffPlus system/services to allow them to live at home. Secondary users are persons who are in direct contact with a primary user. This group is further divided in health care professionals and formal and informal caregivers. Formal caregivers are home care personnel and informal caregivers are close relatives or friends who take care of the primary user.

We have followed the project for a period of three years and focused on understanding what types of privacy requirements were formulated during the development process, which ones were implemented and why they were implemented. Hence, this makes an interpretative approach suitable [15]. Data was collected during these three years by reviewing the project's deliverables, its working documents and the project's blog. A few interviews were also conducted with developers responsible for test sites in Sweden. The collected data was analysed in four steps. First, we identified privacy requirements. Second, we investigated how the requirements were implemented in the system. The requirements could, for instance, be implemented as a technical mechanism or a guideline or not implemented at all. In the third step we compared the privacy requirements and their implementations with the PbDPs defined by [1]. This was done in order to find which PbDPs were applied and which were ignored. We also studied whether the implementations of privacy requirements were in line with the PbDPs. Finally, we investigated the reasons why some of the PbDPs were not applied. An example chosen from the analysis is presented in Table 1. The limitations of the PbDPs identified in the project were then discussed and finally, based on this discussion, PbDPs adjusted for the context of SHSE were suggested.

4 Compliance with PbD Principles - Analysis of the Case Study

Since GiraffPlus aims to collect, store, process and transfer a considerable amount of personal and medical data, privacy and security issues were often raised during the project and the importance of data security and privacy was emphasized during

development of the GiraffPlus system[1]. In the following text we describe how the privacy requirements formulated in the GiraffPlus project and their implementations comply with PbDPs stated as Cavoukian et al. [1].

Table 1. Compliance with PbDPs

Privacy requirement	Implementation	Compliance with PbD	Explanation
GiraffPlus shall allow access to personal data only by authorized personnel and only for legally authorized purposes	An access control system based on passwords. When authorized, the different kinds of users (i.e. health care personnel, therapists, relatives) are able to access all the information about the elderly. Relatives can only access information about their relative, other users, when authorized, can access information about all caretakers	Data limitation (collection limitation principle) which is a key aspect of PbD was not applied	The current implementation was seen as a temporary solution that would be improved in future versions of the system

4.1 Principle 1: Proactive not Reactive; Preventative not Remedial

The first principle emphasizes that respect for privacy should be included before the technology is developed. In the GiraffPlus project the requirements related to privacy were stated and formulated early in the project, before the construction of the GiraffPlus system began, indicating that this principle was followed. The privacy requirements were formulated on a general level, mainly based on the current EU data protection directive 95/46/CE as well as other privacy legislations such as Swedish law for data protection. Compliance with current privacy regulations was emphasized as very important in the project.

However following the documentation of the project we can see that privacy was not in focus when the users' requirements were collected and design principles for the system were formulated[2]. The main goal of the focus groups, questionnaires and workshops was to understand the users' requirements regarding the type of services and parameters to monitor and to study the users' preferences with respect to system design and physical appearance and not their preferences regarding privacy. As it is described

[1] D1.3 System Reference Architecture, D2.1 First Prototype of Sensors, Giraff Platform and Network System.

[2] D1.1 Deliverable 1.1 User Requirements and Design Principles Report.

in the documentation[3] the data privacy and security issues emerged during the focus group and the workshop phases. The concerns raised during these phases were related to the continuous monitoring and access to the data, however practical solutions to these concerns were often postponed to the future and the privacy problems were solved when they occurred during or after the deployment of the system. For instance, very soon after the system was deployed at the test sites, it was discovered that informal caregivers could access too much information about their elderly relative (medical data) and also in some cases they could access information about other elderly persons participating in the projects. The problem was eventually taken care of but as one of the developers put it "it took much more time than expected, resulting in a delay in the project"[4].

To conclude, the development of the GiraffPlus system was functionality-driven and not privacy-driven. Privacy requirements were formulated in the beginning of the project, but on a general level. Their implementation was not focused in the early stages of the development process raising sometimes privacy problems that were taken care of after they occurred. This in turn resulted in delays in the project. One of the reasons for this functionality-driven focus was that defining the system´s functionality was the main objective of the project. Another reason was that it was important to be able to test a functional prototype of the GiraffPlus system in home settings where it is supposed to support vulnerable elderly people. Lacking functionality could jeopardize the elderly persons' safety and security.

4.2 Principle 2: Privacy as the Default

This principle means that privacy protection is built into the system by default and thus the individual does not need to perform any extra actions to protect his/her privacy when interacting with the system. Some parts of personal data processing are automatically protected in the GiraffPlus system. For instance, transmitted and stored data is encrypted and all access to the system is protected by usernames and passwords. However other privacy requirements cannot be implemented in the GiraffPlus system by default because they are highly individual and changeable in time. For instance, one of the privacy requirements of the GiraffPlus system is: "the GiraffPlus system can be installed with a minimum number of sensors which is decided by the users in accordance with the specific monitoring needs (i.e. the ability of customization)"[5]. Hence, the number of sensors cannot be decided beforehand (for instance as a standard solution), but must be decided every time the system is installed at an elderly person's home. Also, it is impossible to decide beforehand where the sensors can be installed and where not. Usually, the bathroom should be avoided for privacy reasons[6]; however, there are situations when the monitoring of these places (constantly or temporarily) might be justified. For instance, during the GiraffPlus project, relatives requested monitoring of their elderly relative's toilets habits. They wanted to monitor how often and for how long the elderly

[3] ibid.
[4] The project's blog.
[5] D1.3 System Reference Architecture.
[6] D1.1 Deliverable 1.1 User Requirements and Design Principles Report.

person visits the toilet. The request was justified by the elderly person's illness. Many such questions were raised in the project indicating the need for personalization of the services and flexibility of the technical implementations. To summarize, some parts of privacy cannot be standardized and built in the technical solution but have to be decided by consulting the elderly person and other stakeholders who take care of that person. The privacy requirements can also change over time and this means that the privacy configurations may need to be changed when the SHSEC is in use. However once the configuration is made the elderly person does not need to perform any extra actions to protect his/her privacy when interacting with the system.

4.3 Principle 3: Privacy Embedded into Design

The third principle says that privacy should be built into the technology. As highlighted in relation to the first principle, privacy and security were emphasized as very important in the context of the GiraffPlus project. Several technical security and privacy safeguards were thus implemented to protect the sensitive personal data during processing, communication and storing. For instance, the technical devices used to build the system, such as sensors, cameras etc. where chosen carefully following the existing security standards and e-health standards relevant for the project[7]. Most of the sensors were provided to the project by the industrial partners i.e. Intellicare and Tunstall. Both these companies provide sensor-technologies that follow the valid standards. Moreover, all the data sent to and stored in the server or kept locally is encrypted with secure and reliable encryption codes[8]. Further, in order to guarantee maximum privacy, a private cloud using existing PaaS open source infrastructure was established[9]. Finally, to ensure the confidentiality of data processed in the system, a two layer approach was used. A certificate consisting of a public and a private key is created by the GiraffPlus VPN Certificate Authority, which enables encrypted communication with other computers in the GiraffPlus Virtual Network. To secure communication with the Web Service, the GiraffPlus Certificate Agency is deployed, which creates public and private key pairs for all components and servers in the GiraffPlus ecosystem[10].

The limitation of this principle in the context of the project is that not all aspects of privacy can be built into the technology. As highlighted in relation to the second principle, there are some privacy requirements that cannot be built into the technology. For instance, the requirements related to the number of sensors installed in the home environment or the position of the sensors and of the Giraff-robot. Since these aspects cannot be built in the technical solution, they need to be regulated differently for instance by complementing guidelines for implementation for the SHSEC.

[7] D1.2 Technological Component Specifications, http://www.giraffplus.eu/.
[8] D1.3 System Reference Architecture, D2.2 Second Prototype of Sensors, Giraff Platform and Network System, D3.1 Context Inference and Configuration Planning Prototypes.
[9] D4.1 The Interaction and Visualization Service and Personalization Module Alfa Release.
[10] D2.2 Second Prototype of Sensors, Giraff Platform and Network System.

4.4 Principle 4: Functionality—Positive-Sum, not Zero-Sum

The fourth principle means that privacy is an integral part of the system without diminishing its functionality. In the GiraffPlus project, the privacy requirements were formulated in the beginning of the project and were partially treated during the whole development lifecycle of the system going from identifying the end users' needs until the evaluation of the user experiences of the system in its real settings. However, the privacy requirements were not treated as equally important as the services offered by the GiraffPlus system. As we argued in relation to the first principle the project was functionality-driven and defining the main services of the system was always the major focus even if it sometimes meant neglecting privacy. For instance, in the GiraffPlus system both health care professionals (doctors, nurses) and formal caregivers (social assistants, occupational therapist) could access all the data collected by monitoring both physiological as well as environmental parameters at the elderly person's home. According to the collection limitation principle (included in principle 4), the personal data should not be disclosed in a larger extent than necessary for the given and clearly specified purpose. The problem in the project was that the purpose and need for monitoring of the different psychological and environmental parameters was not yet clearly decided. Finding what is relevant to monitor and for what purposes was a part of the research activities of the project. Second, the current implementation was seen as a temporary solution that should be improved in the future versions of the system, since there was only a limited number of secondary users who tested the system. The focus in the project was to make the system work; thus, the functionality was prioritized before privacy.

4.5 Principle 5: End-to-End 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). In relation to the GiraffPlus project, this principle means that the right amount of data is collected for a clearly stated purpose, that data is protected during processing, transition and storage and that it is decided where and for how long the data is stored. In relation to principle 3, we described what security measures were implemented to ensure confidentiality of the data processed by the GiraffPlus system. It can be concluded that all sensitive data processed by the system is protected during some parts of the life cycle. The problem with this PbDP in the context of the project is that it is still unknown how the system will be used in practice in the future. During the project, the system was evaluated in home environments, but it was only partially tested by the secondary users (healthcare professionals, formal caregivers and informal caregivers). Thus it is unknown what consequences the implementation of the system can have on privacy in the future use. Many questions related to privacy remain unanswered. For instance: where should the data that is collected through the SHS be saved? Should it be part of the elderly's records or should it be saved somewhere else? How long should the data be kept in the system and for what purpose? How should the data be interpreted? They are important questions that need to be answered before the SHS is implemented.

In the project documents[11], the problem of lacking legislation regarding eHealth in general is also highlighted. It is argued that unclear regulations make it difficult to clearly decide the rules for how sensitive data should be handled when the SHS is in use. It can thus be concluded that in a development project such as GiraffPlus, it is difficult to take care of privacy concerns that may arise when the SHSEC is used in real settings i.e. as a part of regular elderly care.

4.6 Principle 6: Visibility and Transparency

The sixth principle states that data protection should be open to independent examination. This means that the different components and operations should remain visible and transparent to users and providers. In relation to a SHSEC, this principle means that the primary user knows (or can find out) what data is being collected, how the data is being used, and who can access it. In relation to this principle, the users' participation is also emphasized, meaning that the users should be included in deciding about the extent of monitoring and about who will be able to access the collected data.

To involve users in the development process was very important in GiraffPluss project. Significant efforts were made to collect and understand user requirements and preferences regarding the type of services and the system design[12]. Although the focus in the project was on defining the system's functionality and not on understanding the users' preferences regarding privacy, such preferences also emerged during the focus groups meetings, questionnaires and workshops. These privacy preferences were then translated to technical requirements of the system. Users were also involved in the configuration of the GiraffPlus system before the system was deployed at their homes and questions regarding privacy were raised during the evaluation of the system. It was also important to obtain a written permission from the primary users before the system was deployed. Therefore it can be concluded that in GiraffPlus project, the primary users were involved in the design process and they could decide about extent of monitoring that is in line with the sixth PbDP.

A difficulty concerning the elderly users´ participation in the design of the GiraffPlus system was related to their insufficient computer skills and their lacking understanding of the technology involved. In the GiraffPlus project, the developers used different methods to improve the elderly's understanding of the technology and of the consequences the system could have on their lives. For instance, the developers used mock-ups in order to increase the elderly's understanding of how they could use the GiraffPlus robot in their homes. Scenarios for the GiraffPlus system were also used to aid to the communication and to increase the elderly peoples' understanding of the functionality in the system[13]. Despite all these efforts the elderly users, who had the system installed at home, were surprised when they could see what data about them and their homes were collected by the GiraffPlus system (interview with a developer responsible for test sites in Sweden). They explained that they did not understand that it was possible to measure

[11] D1.1 User requirement and Design Principles Report.
[12] Ibid.
[13] D6.1 Preliminary Evaluation Report.

all these parameters using the sensors. They thought that it was only possible by using video cameras. Thus to comply with this PbDP is a challenge in the context of SHSEC because the elderly people have difficulties in understanding the consequences of the implemented technology on their privacy. It was also recognized that in some cases, other stakeholders (relatives, formal caregivers, health care professionals) decided what was relevant to monitor and to what extent without involving the elderly person him/herself. This is also seen as problematic in relation to this PbDP.

4.7 Principle 7: Respect for the Users' Privacy

This principle means that the individual's privacy should be an interest of designers and operators of health systems. As we described earlier, ensuring privacy of the primary users was a high priority during the GiraffPlus project. Thus the users' personal data collected during the project was treated according to current laws and regulations. However, it was recognized during the project that the different stakeholders involved in the design of the GiraffPlus system (developers, health care professionals, formal caregivers, informal care givers) could have different opinions regarding privacy and functionality and could focus on different aspects in this context[14]. For instance health care professionals and system developers most often focused on standardized privacy regulations and preferences that can be applied to the whole population, while caregivers put more attention to what was important for the elderly people they take care of. The general privacy demands are easier to build in the system as default, while the individual needs must remain to be flexible.

5 PbD Principles in the Context of SHSEC

In the previous section several limitations of the PbDPs in the context of the GiraffPlus project were highlighted. In this section, based on this discussion we suggest a set of PbDPs that complement the existing PbDPs and make them more appropriate for the context of SHSEC.

Principle of Holistic Thinking. We described in the case study section that not all aspects of privacy identified as important during the GiraffPlus project could be built into the technology (see Sect. 4.3). Holistic thinking aims at advancing the third PbDP, namely privacy embedded into the design. Although the third principle stays that the privacy must be embedded into the design and architecture of IT system and *business practices*, the focus when applying this principle is all too often on finding technical safeguards that can protect the sensitive data from unauthorized access when processed by the IT-system. This represents a very narrow view on privacy and clearly ignores the other aspects of privacy, such as installing the technology in different parts of the home, choosing the appropriate monitoring technology and the level of detail up to which activities can be monitored. Thus we suggest a principle of holistic thinking.

[14] D1.1 User requirement and Design Principles Report.

This principle means that privacy in the context of SHSEC include also aspects beyond data protection that must be considered to be able to ensure the privacy of the elderly person when using a SHSEC. Therefore the measures implemented to protect the elderly person's privacy in the context of SHSEC cannot be limited to technical safeguards. Equally important is establishing adequate procedures and business practices.

Principle of Flexibility. As it is described in the case study section, the elderly person's health situation can change over time and certain privacy-invasive functionality may (no longer) be necessary. Also the elderly person's privacy requirements may change over time and something that was accepted in the beginning may no longer feel comfortable. Hence, we suggest a principle of flexibility. This principle means that privacy implementations in a SHSEC should be adaptable and capable to change over time. This principle is an advancement of PbDP 7: Respect for users' privacy and principle 1: Proactive not reactive; Preventative not remedial.

Principle of Personalization. In the case study section we showed examples of the differences between the elderly users' needs, preferences and expectations. Acknowledging these differences is important to be able to support independent living and ensuring the privacy of the elderly person. Therefore, we suggest a principle of personalization. This principle means that the elderly should have a right to an adjustment of the offered solution (SHSEC) to his/her individual needs and preferences. This principle also means that the SHSEC needs to be configurable due to handle the huge heterogeneity across elderly users. In other words the elderly should have a right to choose the services (time and length of the monitoring) and technologies used (cameras, sensors) according to his/her individual needs and wishes. This principle is an improvement of PbDP 7: Respect for users' privacy.

Principle of Empowerment. The users' involvement in formulating privacy requirements is emphasized in PbD (especially in PbDPs 1, 6 and 7). In the GiraffPlus project special efforts were made to involve elderly users during the design of the GiraffPlus system. However, we could see that sometimes the elderly were persuaded to accept the requirements of the other stakeholders (i.e. the secondary users, relatives), which is not that difficult because the elderly are in a vulnerable position since they are in need of special care, have very low experience with and knowledge about the technology. Therefore, there is a need of empowering elderly people and give them sufficient means to be able to formulate their privacy preferences and to give informed consent regarding time and extent of monitoring services. Thus we suggest a principle of empowerment. This principle can be applied with help of the principle of clarity and the principle of control, described below.

Principle of Clarity. SHSEC involve smart but complex technologies. The different functions of the system are negotiated with the elderly, but they often do not fully understand what they agree to. In the early stages of the design, the system is very abstract and hence, the lack of sufficient (technical) knowledge and awareness makes it difficult if not impossible) to properly assess the consequences on the privacy. Therefore, there is a need for introductory presentations, special methods for collecting the elderly's

requirements and usage scenarios that visualize the impact on one's privacy when the system is used. Several of such methods have been successfully used in the GiraffPlus project (as described in the case study section). Thus we suggest the principle of clarity that means that it should be understandable and clear for the elderly what services are implemented, how the data is collected, when and where they are monitored, who has access to the collected data and how the collected data is interpreted. All this aspects should be communicated to the elderly user in a clear way. This principle is an improvement of PbDP 6 and 7 and complements the principle of empowerment presented above.

Principle of Control. Based on the findings from the case study we suggest also the principle of control. This principle means that the elderly should feel that they have control over their life, the implemented technical devices and the data that is collected about them by the SHSEC. To respect this right, formal approval by the elderly regarding these previously mentioned aspects should be required. It is also important that the elderly has a right, capability and/or knowledge to switch off the monitoring when he/she wishes to do so and if it does not jeopardize his/her safety and security. This principle is an improvement of PbDP 6 and 7 and complements the principle of empowerment described earlier.

Principle of Privacy Management in Use. One considerable problem when applying the existing PbDPs during the GiraffPlus project was caused by the fact that the GiraffPlus system was seen as a prototype and therefore, the implementation of the privacy requirements were postponed to the future when the system would be commercialized. Although PbDP 5 emphasizes the importance of considering privacy aspects arising after the system have been developed, this principle is difficult to apply in the context of SHSEC because of lack of experiences, knowledge and regulations with regard to the use of SHSEC in practice. Therefore we suggest the principle of privacy management in use which is an improvement of PbDP 5. The principle of privacy management in use means that privacy aspects regarding the use of SHSEC in real settings should be considered already during the development of SHSEC. It can be done by involving significant stakeholders, such as health care professionals, formal and informal caregivers, politicians in development of a SHSEC. Privacy aspects that may appear when the current SHSEC is in use can be discussed with these stakeholders by using future usage scenarios of the system.

6 Conclusions and Future Research

As argued in the literature, ensuring privacy of the elderly is one of the main concerns in the design of SHSEC. PbD, which helps to build in privacy in technical specifications of IT systems, is seen as a possible solution to this problem. In this paper, we investigated the suitability of existing PbDPs [1] in the context of SHSEC. Through a thorough analysis of the case study, we have identified several limitations of existing PbDPs in this context. Based on these findings, we have suggested seven additional PbDPs which complement Cavoukian's et al. [1] PbDPs and adapted them for the context of SHSEC.

The complementing principles suggested in this paper are based on analysis of a case study. In the future research that is already in progress, we discuss these principles in relation to existing literature in order to find if the experienced limitations were project-specific or if they are general in the context of SHSEC. Based on this discussion we aim to further develop and validate the suggested PbDPs.

References

1. Cavoukian, A., Fisher, A., Killen, S., Hoffman, D.: Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design. Ident. Inf. Soc **3**, 363–378 (2010)
2. Alam, M.R., Reaz, M.B.I., Ali, M.A.M.: A review of smart homes - Past, present, and future. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **42**, 1190–1203 (2012)
3. 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)
4. Demiris, G., Hensel, B.K., Skubic, M., Rantz, M.: Senior residents' perceived need of and preferences for "smart home" sensor technologies. Int. J. Technol. Assess. Health Care **24**, 120–124 (2008)
5. 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 Inf. Med. **48**, 29–37 (2009)
6. Li, K.F.: Smart home technology for telemedicine and emergency management. J. Ambient Intell. Humaniz. Comput. **4**, 535–546 (2013)
7. 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 Ment. Health **15**, 419–427 (2011)
8. 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)
9. Nordgren, A.: Privacy by design in personal health monitoring. Health Care Anal. **23**(2), 148–164 (2013)
10. Kosta, E., Pitkänen, O., Niemelä, M., Kaasinen, E.: Mobile-centric ambient intelligence in Health- and Homecare-anticipating ethical and legal challenge. Sci. Eng. Ethics **16**, 303–323 (2010)
11. Bowes, A., Dawson, A., Bell, D.: Implications of lifestyle monitoring data in ageing research. Inf. Commun. Soc. **15**, 5–22 (2012)
12. Frennert, S.A., Östlund, B.: Review: seven matters of concern of social robots and older people. Int. J. Soc. Robot. **6**, 299–310 (2014)
13. Lowe, S.A., ÓLaighin, G.: Monitoring human health behaviour in one's living environment: a technological review. Med. Eng. Phys. **36**, 147–168 (2014)
14. Steele, R., Lo, A., Secombe, C., Wong, Y.K.: Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. Int. J. Med. Inf. **78**, 788–801 (2009)
15. Myers, M.D.: Qualitative research in business & management. Sage Publications, London (2009)