Privacy Concerns in a Remote Monitoring and Social Networking Platform for Assisted Living

Peter Rothenpieler, Claudia Becker, Stefan Fischer

Privacy concerns in a remote monitoring and social networking platform for assisted living

Peter Rothenpieler, Claudia Becker, and Stefan Fischer

Institute of Telematics, University of Lübeck, Germany
{rothenpieler,becker,fischer}@itm.uni-luebeck.de
http://www.itm.uni-luebeck.de/

Abstract. In this paper, we present an online platform for the field of Ambient Assisted Living (AAL) which is designed to support a self-determined and safe life for elderly people in their own homes instead of admission to a nursing home. This goal is achieved through in-home monitoring of the clients using wireless sensor networks in combination with a social networking approach based on personal Patrons. The platform further acts as a marketplace for third party service providers which can extend the functionality of the platform, supplying the users with individual made-to-measure assistive services. This paper provides an overview of the concept behind this platform with special focus on privacy issues.

Keywords: Privacy, Ambient Assisted Living, AAL, Monitoring, Sensor Network, Social Network, SmartAssist

1 Introduction

According to figures from the *Statistisches Bundesamt* (see [1]), the number of people aged over 65 in Germany will increase from 19% to over 30% in the next 50 years, preceded by an increase of people in need of medical care by 58% already in the next 20 years. This phenomenon will not only be limited to Germany since many other countries especially in Asia and Europe are facing severe population ageing in the near future, e.g. Japan, Italy and Spain [2]. All around the world, population ageing will thus lead to an overall increase in the costs of healthcare and annuity in the next 20 to 50 years, but at the same time may cater towards profitable services which increase the quality of life for elderly people.

The project described in this paper belongs to the field of Ambient Assisted Living (AAL) and aims at creating an online platform that is designed to support a self-determined and safe life for elderly people in their own homes. It is targeted at providing needs-based care by personal Patrons through the use of remote accessible in-home sensor networks and an online social networking platform. Since Patrons can be represented by relatives, medical doctors and friends, as well as commercial service providers, several privacy issues arise out of this context.

The proposed system aims at postponing the admission of elderly people to a nursing home to achieve permanent monitoring. As mentioned in the work of [20], "the loss of privacy is significant when elderly persons are admitted to nursing homes, where they are likely to become permanent and often dependent residents". In a nursing home, the staff members are required to care for residents' intimate personal functions, e.g. in a common shower or tub room. In [20] it is further stated that "although actions to protect residents privacy are viewed as important, staff members may passively accept the premise that privacy as a right and as a norm is not feasible [...] for getting the work done".

In the course of this paper, we will describe the concept and architecture of our service portal in more detail and also identify issues regarding informational self determination as well as the protection of personal information. We will give an overview of related work in the field of social networks and data privacy and will conclude in the last section with an outlook on the steps to be taken in the future.

2 Concept

This section contains an overview of the concept and architecture of the service portal and a description of the two main user groups, *Seniors* and *Patrons*. The web based service portal is used to provide the user with increased personal safety, independence, better means of communication as well as easier social interaction and an extendable set of individual assistive services. The basis for this support consists of two data sources: Personal data entered by the user on the one hand and automatically generated data measured by an in-home sensor network on the other hand. This information is aggregated and analysed at the service portal, as depicted in Figure 1, and made accessible to the Patrons, family, friends and service providers of the user, if granted. To provide the user with increased safety, Patrons can monitor the automatically generated sensor readings in combination to the rich information available through the social network like e.g. recent activities or habits of the user. As mentioned above, the users can be divided into two main groups - the Seniors and the Patrons:

In SmartAssist, Seniors are elderly people of age 65 or above, who are either retired or unemployed and thus spend a large amount of time in their own apartments. Seniors considered in this work are further set to have a score of at least 23 points at the MMSE (mini-mental state examination / Folstein test) and thus do not suffer from dementia or cognitive impairment yet. Demographic characteristics include the following: According to [3], more than 60% of people aged 65 to 80 are women, increasing to more than 70% beyond the age of 80, while 18% of people aged 65 to 70 are single-person households, increasing to 53% for people in the age of 80 to 85 according to [4] and [1]. The group of Seniors can further be characterized by their motivation for using the platform. On the one hand, Seniors can be interested in preventive care and thus use the system for early detection, diagnosis and prevention of diseases and disabilities (group 1.1.3 in [5]). On the other hand, Seniors are people in need of assistance (group

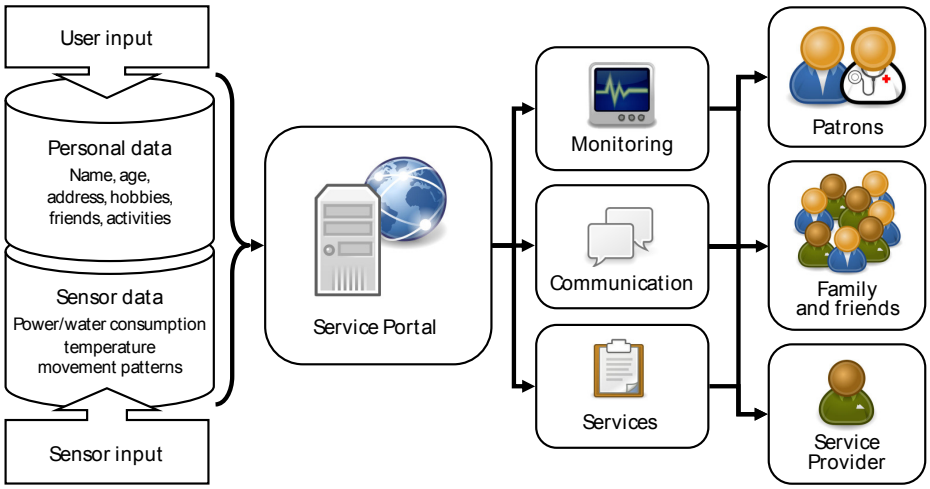

Fig. 1. Architecture overview

1.2 in [5]) who are willing to use the services provided through the platform, or both.

The role of a Patron can be played by a variety of groups, ranging from family members, friends, neighbours, medical personnel or professional care providers. The first of these groups can be characterized as *caregivers* or *healthcare assistants* (group 2.1.1 in [5]) like children, grand-children or siblings who can watch over the user or close friends or neighbours who can periodically check if everything is in order. The group of *medical personnel* (group 2.2 in [5]) like doctors, physicians and paramedics will act in the role of a Patron and monitor or diagnose the medical condition of the user. Third party service providers (group 2.4 and 3.8 in [5]) such as security companies, domiciliary care providers or ambulance services may also be incorporated as Patrons for taking immediate action in the case of an emergency.

The service portal can be divided into three main functional components which are the monitoring component, the communication component and the services platform, as seen in Figure 1. We will describe each of these components in more detail in the following subsections.

2.1 Monitoring

The monitoring component of the online portal displays all information gathered through the in-home sensor network to the Patrons and gives warning in the case of sudden or subtle changes in the readings. The sensor network gathers information about the daily routine of the Seniors by continuously monitoring the electric power and water consumption, the opening and closing of doors as well as observing ambient temperature and humidity.

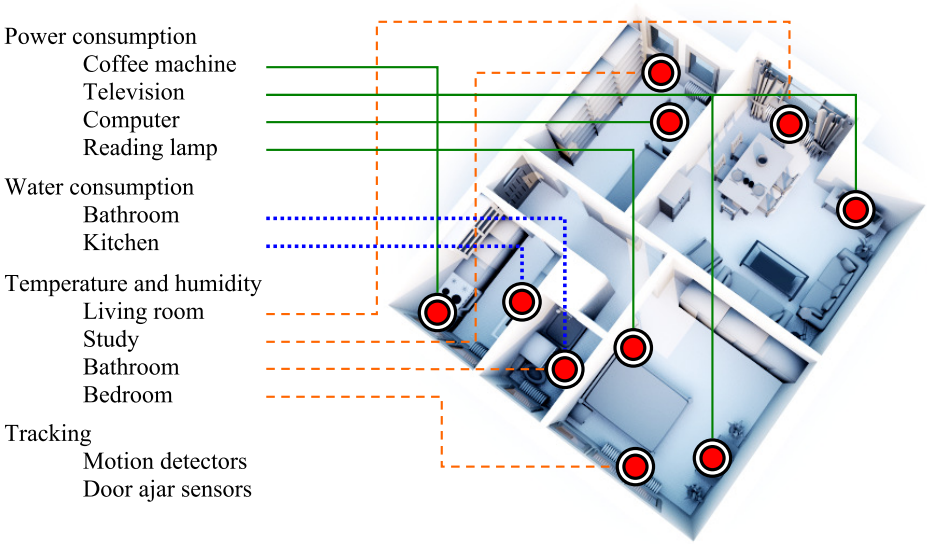

Fig. 2. Domestic sensors

The following examples are used to outline the information which may be gained through the analysis of the temporal changes in the readings of the in-home sensors. The significance of the following indicators has not been analyzed yet as this will be subject of field tests performed in the course of this project. These indicators merely serve as examples for the quality of information collected about the users which will be discussed in Section 3.

Figure 2 shows the sensors located in the home of a prospective user as follows:

Monitoring the power consumption of the coffee machine in the kitchen and the reading lamp in the bedroom is used to indicate the circadian rhythm or sleep-wake cycle of the user, while the consumption of the computer and television can provide information about his daily routine and activities. The amount of water consumed in the bathroom can e.g. be used to monitor the usage count and frequency of the water-closet. In combination with the subsequent water consumption at the lavatory, this can further be used as an indication for the personal hygiene of the user. The ambient temperature and humidity in every room and its temporal change can be used to monitor heating and ventilation in the apartment. This can not only be used to show the actual temperature but also to indicate the perceived temperature or heat index (HI).

The sensor readings are gathered by the sensor nodes and transmitted to a residential gateway, via a wireless connection. To protect the transmitted information against eaves-dropping or manipulation, the communication between sensors and gateway is encrypted along with authentication and integrity protection. The residential gateway stores and continuously forwards the sensor

readings to the service portal via an existing Internet connection using HTTPS. Gateway and server both feature digital signal processing and pattern recognition software components to generate an alarm in case of an emergency which will then be sent to the Patrons using Short Message Service (SMS) or E-Mail and being displayed in the service portal. To reduce the incorrect classification of sensor readings, the sensor network repeatedly undergoes a (re-)training phase in each apartment in which the signal processing and classification algorithms are primed to its specific environmental conditions. These components are not part of the service portal and thus beyond the scope of this paper.

2.2 Communication

The online portal acts as a frontend for the communication and exchange of experience and information between all users of the platform, Seniors and their Patrons alike. While being comparable to online social networking sites like e.g. Facebook or MySpace, the proposed platform focuses on the personal relationship between the elderly people and their personal Patrons.

The use of social networks in assisted living systems is also proposed in [18]. In their work, the authors argue that even though elderly people tend to live alone, they should live embedded in a caring personal network. According to [18], "this is the most effective way to ensure [...] longevity [...] (and) a good quality of life in the face of high probability of chronic physical and cognitive impairment".

The service portal offers social networking features like profile creation, photo sharing and a messaging service. The Patrons and service providers can use the information stored in the user's profile, like name, age and hobbies, as metadata for the diagnosis in the remote monitoring component. Especially data about recent activities or mood of the user available through a micro-blogging feature comparable to the Facebook Newsfeed ("What is on your mind?") could prove to be useful for medical diagnosis. Emotional conditions such as stress or depression or physical conditions such as headache or tiredness can hardly be monitored through the sensors but may be available to the Patrons if the user enters them in his profile.

Social information may further not only be useful for medical purposes but can also help to protect the privacy of the users. In their study [20] on personal privacy in a nursing home, the authors analyze the interaction between staff and residents and suggest that privacy violations occur more easily with increasing degree of depersonalization and create less guilty conscience among the violators. According to [20], depersonalization was reduced through presenting pictures and stories about the residents' past. The authors summarize this as: "Respect for privacy was respect for the person revealed in those pictures and stories". In the social network proposed in this paper, Patrons who are not already personally involved with the Seniors, are supplied with photos and stories. This personal information may in turn help to reduce the above mentioned degree of depersonalization and thus help to increase the protection of the Seniors' privacy.

Even though the portal focuses on the relationship to their Patrons, users may also interact with each other and their individual peer groups. The use of messaging services, interest groups or event calendars may increase the social interaction between the users and their relatives, friends and local community. Through the use of messaging and photo sharing or virtual tea parties, the enhancement of social interaction across distances or for people with disabilities could be achieved. Interest groups or event calendars on the other hand can be used as sources of information about local sports events, garage sales or casual game tournaments which can strengthen the participation and integration of the users into their local community and therefore decrease their social isolation.

2.3 Services

The aforementioned service providers are not limited to the role of a Patron but can also use the platform as a marketplace to offer their own services. Just like modern cellphones can be extended in their functionality through the *Android Market* (Google Inc.) or *App Store* (Apple Inc.) by third party software, the portal allows the incorporation of user-centric services from independent providers. Users are given the choice to grant access to personal information and sensor readings to certain services which in turn produce additional benefit to the user.

Services for the target user group of elderly people include e.g. timetables and ticketing for public transportation, "Meals on Wheels" with a menu customized for each user's needs along with rating functions providing direct feedback on the quality of the meals to other users. On the other hand, services that health insurance companies could be interested in may be the creation of anonymized statistics about users. Services comparable to the one demonstrated in [6], where a sensor-enabled blister watches over the medication of a patient, are also likely to be integrated into the platform.

Depending on the individual use case of each service, the usage of the service may be free-of-charge, financed by advertising or require a monthly fee. Instead of advertising, services may also be partly or fully financed through the health insurance companies, either as a form of health care or prevention or by letting the insurance company collect statistical data about the users. Reduced monthly fees for insurances or the opportunity to collect bonus points that in turn can be exchanged for future prevention or treatment may encourage users to install and participate in third party services.

3 Privacy

The use of social networking sites alone often leads to a variety of privacy and safety concerns. Examples include the stealing and selling of user data such as e-mail addresses, passwords and personal data for spamming or phishing as well as identity theft crimes. Since these sites often contain more than just general information about people like names, addresses and dates of birth, e.g. also photos of users and friend lists, identity theft has become considerably easier and

automatable. In the work of [7], an automated attack mechanism is proposed, in which existing user profiles are cloned. The authors also describe how profile information can be collected through sending friend requests to the contacts of the cloned victim. This can then obviously be extended to cross-site cloning of these profiles and so on. Given the fact that today already more than 400 Million users are active on Facebook every day [8], there is a big potential for this kind of attacks and especially inexperienced users are easy targets.

The proposed online portal, which contains even more information about the users, including medical or behaviour pattern information, thus is an even more attractive target to attacks because it contains worthwhile information. We will describe the security threats and privacy concerns for each platform's component in the following subsections.

3.1 Monitoring

Even though the monitoring component is targeted at fulltime surveillance, the user's privacy has to be respected and thus total control over individual sensors and the system as a whole has to be granted to the user himself. The user needs to be enabled to make use of his right on informational self-determination - i.e. take control on which data is collected at any time, and the opportunity to view, edit and delete the data which has already been collected. In case the privacy of the user and his visiting guests is not dealt with correctly, this may very likely result in a lowered system acceptance by the user. This may also increase the user's social isolation if his friends refuse to enter the bugged apartment.

To accomplish this, every sensor needs to be equipped with an easily accessible on/off switch and a status indicator in combination with a global privacy switch, e.g. located at the entrance door. A reasonable extension of this manual override could include a scheduling system which can be set to privacy mode on planned occasions/appointments in the future or even an automatic system which detects the presence of visitors when entering the user's apartment. The user further needs to be able to view all collected data and to edit incorrect information or to delete unwanted information without any restrictions or consequences.

The collected data about the user has to be minimized to the amount which is required to effectively fulfil the monitoring task. This will result in the adjustment of the sample rate on the one hand but may also include different mechanisms for data fuzziness. Fuzziness may be achieved through the use of high-pass or low-pass filters or by adding a (reversible) noise signal comparable to the Selective Availability feature of GPS. The data further should be kept anonymous as long as possible and should only contain references to the originating household if this information is needed, e.g. by an ambulance. The use of wireless sensor nodes instead of primitive sensors offers the possibility of in-network analysis and processing of data.

In contrast to the user's control over the system, the system has to be secured against external attacks. The communication between the sensor nodes in the user's apartment and the gateway as well as the communication between the

gateway and the service portal has to be secured. All transmitted data has to be protected against manipulation, eavesdropping or man-in-the-middle attacks. The communication thus needs to be encrypted using similar means as WPA2 for IEEE 802.11 and may face similar attacks, like e.g. wardriving. If an attacker is able to gain access to the sensor data of a specific household, similar attacks such as described in [9] may be used to plan a burglary through prediction of the user's presence in his apartment.

3.2 Communication

The communication component contains the user interface and lets the user enter, view, edit and delete his personal information along with the sensor information as described in Section 3.1. In addition to the adequate presentation of this information, the user interface needs to provide means for the user to control the access rights to the private information and to be capable of informing or warning the user about which information is currently accessible to or accessed by whom.

The definition of access rights through the user needs to be accessible in terms of conformance with standards such as the WCAG[1] of the W3C's WAI[2] or the German BITV[3] but also needs to be comprehensible for the target audience of users aged 65 and above as described in Section 2. While the accessibility can be reviewed through automatic tests like [10] the suitability or usability for the target audience cannot.

The usability of the privacy settings needs to be based upon the use of restrictive default settings (hide-all) which prevents information leakage through in-action of the user. Instead of sharing the information itself, configurable views which contain the shared information, comparable to business cards, may be used. These views should be both owner- and viewer-accessible and may as well include disinformation about the user, depending on the specific viewer or purpose of sharing. The user interface should further protect the user's information through the use of warning messages, in case confidential information is about to be shared involuntarily or unknowingly. These warning messages need to be unobtrusive and not annoying for the user, to avoid that the user ignores or even deactivates this security mechanism.

Even though the information needs to be protected against illegitimate access while at the same time being fully accessible to the user who is the owner of this information, there are certain circumstances under which the user himself should be protected from accessing his own information. Along with the right of informational self-determination, it is commonly accepted [21] that the user has the right of nescience (unknowingness). Given, for example, the automatic diagnosis of a disease through the service portal, this information should not be accessible instantaneously to the user. Instead, this information should be

[1] Web Content Accessibility Guidelines
[2] Web Accessibility Initiative
[3] Barrierefreie Informationstechnik-Verordnung

communicated through the use of a human intermediary such as the user's family doctor. The computer system lacks the ability to correctly inform the user about the actual chance of the diagnosis' correctness and its consequences while not being able to judge if the user actually wants to be informed about this special diagnosis. Reasons for this nescience do not have to be provided by the user, but can include an existing advance directive or financial and legal consequences of the user towards his insurance company.

Comparable to the communication described in Section 3.1, the information exchange between the user's personal computer, which is used to display the user interface, and the service platform need to be secured using mechanisms like HTTPS to ensure data confidentiality and integrity protection as protection against eavesdropping, manipulation and man-in-the-middle attacks.

3.3 Services

The incorporation of external services into the platform is targeted at providing additional safety or benefit for the user through third party extensions. Access to the user's personal information and sensor readings must be secured and restricted by external service providers in the same way as mentioned in the previous Section 3.2 but faces additional security and privacy concerns. Due to the external nature of these services, all data which once has been transferred is no longer under direct control of the user but of the service provider. Therefore, the user must be informed explicitly about the data which is available to the external services and which information has been transferred to whom. The external service providers must in return be forced either through technical means or at least be obligated to take measures by themselves to ensure that the information is protected. This can be achieved in the form of a Terms of Use Agreement which should be presented in a layered complexity fashion, reflecting the user's capabilities and willingness to read multiple pages of legal text. This includes that information is not passed on to other external parties and that information is used only for the specific purposes accepted by the user. Data access for the external providers must therefore be supplemented with a secure and authenticated logging function which must also include the possibility for the user to revoke, delete or alter transferred data without any restrictions.

Comparable to the use of views described in Section 3.2, the user may as well provide disinformation about him to the external services. The forging of information in this case is not only limited to personal information but may also include virtual or physical tampering with the sensor readings. The readings should be protected from physical tampering and the platform should include a form of virtual tampering, i.e. uncertainty/privacy enhancement features where a user can control the degree of privacy which is added to the data before transmitting it to the service provider. Properties such as authenticity, uncertainty and precision of sensor readings must be determinable to the service provider e.g. in form of a "similarity-index" to the original data in case the sensor data is used for insurance measures. In contrast to the concept of identity theft in-

troduced in Section 3, the concept of sensor data theft could otherwise result in an insurance fraud.

4 Related Work

The domain of social networks with focus on elderly people already features a variety of different approaches, especially in the USA. Examples for these networks include conventional approaches like Eons.com [11] which was launched 2006 and features game, photo and video sharing components and provides its users with information about topics like health, relationships, fitness, debt, retirement and insurance in the form of interviews and articles. Online platforms like PatientsLikeMe [12] and DailyStrength [13] on the other hand focus on people which share the same disease or face the same problems in their lives. These platforms allow their users to exchange information and experiences about symptoms and treatments of their diseases or strategies and emotional support for people dealing with e.g. depressions, a divorce or midlife-crisis. The online community MedHelp.org [14] features discussion boards on health related topics and cooperates with medical doctors and physicians for "finding cures together" and, according to information available on the website, is visited by more than 10 million people each month.

Along with the increasing amount and availability of personal information through these online platforms, the manageability of access control needs to be increased. The users on the one hand need to be informed about which information is accessible to whom, including the provider of the platform and subscribed services. On the other hand, they need to be able to use the platform's privacy settings correctly.

The work of Vu et al. [15] presents a study on how users read online privacy policies and how well those policies are understood by their readers. The authors investigate the user's abilities to recall information after reading a policy or to search for information within the policy in response to specific questions. It is stated that regardless of whether the participants were allowed to search the policy while answering the questions or not, the comprehension scores were still low across all participants, featuring only 42% to 55% correct answered questions. The authors conclude that important information in privacy policies is not stated in a way that can be easily understood by users. In addition, the way that privacy relevant information is presented, is confusing to the users. The fact that the participants of this study were in their twenties and experienced with computers and the Internet and further either graduate or undergraduate university students, shows that even experienced users struggle with online privacy policies. To overcome the problem of privacy policy complexity for the user, the use of Agents for Privacy-Preference Specification is proposed in [16], which in our use-case could include the concept of Patrons in addition to or instead of Agents. Agents or Patrons alike could in term help the user specify or correct his privacy settings.

Explanations as to how and why users make decisions to share or protect their personal information on the social networking site Facebook is given in [17]. This study demonstrates that even though users are aware of the publicity of their profiles and attempt to disclose sensitive information, the user's privacy decisions are not reflected upon very often. Once the privacy settings of a user are configured, e.g. on account creation, the users only changed their settings after noticeable and disturbing events, such as a privacy intrusion. It is mentioned further that users often disclose information to a broader audience than really intended, e.g. through their wall posts. The authors suggest solutions to these problems which include enforcing more restrictive privacy settings as well as more restrictive default settings. They also demand for improved user interfaces which provide a more accurate mental model of the outcomes of the user's settings and actions.

5 Conclusion

In this paper we presented the current status of one of the components of the SmartAssist project. Development of the proposed service portal will continue in the following months, culminating in the deployment of the system in several households in the city of Lübeck, Germany, in the next two years. The goal of this field test will be to test the medical benefit for the user and the significance of the indicators mentioned in Section 2.1.

Our next step, prior to the field test, will be to identify the Seniors needs and requirements in user surveys and interviews. The goal of this analysis will be to pinpoint the most important features for assisting the Seniors with their daily activities from their perspectives. During the field test we will continuously improve our system, considering content and user-experience issues as mentioned in [19]. Special attention will be paid to the privacy concerns raised in Section 3 and the usability of our proposed system will be tested regarding these concerns. The corresponding privacy mechanisms will be expanded to meet the expectations and needs of the users as well as new concerns arising during deployment.

Acknowledgements. This paper is part of the research project SmartAssist funded by the Federal Ministry of Education and Research, Germany (BMBF, Förderkennzeichen: 16KT0942). SmartAssist belongs to the research area of AAL and is a joined project between the University of Lübeck, the Vorwerker Diakonie, coalesenses GmbH and the Lübecker Wachunternehmen.

References

1. Peter Georgieff: Ambient Assisted Living - Marktpotenziale IT-unterstützter Pflege für ein selbstbestimmtes Altern. In: FAZIT-Schriftenreihe Forschung, Band 17 (2008) ISSN:1861-5066, MFG Stiftung Baden-Württemberg, Fraunhofer ISI, 2008

2. Percentage distribution of the population in selected age groups by country, 2009 and 2050. In: World Population Prospects, The 2008 Revision, Summary Tables / Annex Tables, pages 2226. United Nations, Department of Economic and Social Affairs, Population Division, 2009
3. Statistisches Bundesamt. Bevölkerung und Erwerbstätigkeit, Sterbetafel Deutschland, 2008
4. Menning, S.: Haushalte, familiale Lebensformen und Wohnsituation älterer Menschen. In: GeroStat Report Altersdaten 02/2007. Berlin: Deutsches Zentrum für Altersfragen, 2007
5. Birgid Eberhardt: Zielgruppen für AAL-Technologien und Dienstleistungen. In: AAL Kongress- und Fachbeiträge. AG Kommunikation, BMBF/VDE Innovationspartnerschaft AAL, 2009
6. Brandherm et al.: Demo: Authorized Access on and Interaction With Digital Product Memories. In: 8th Annual IEEE International Conference on Pervasive Computing and Communications. PerCom-2010, March 29 - April 2, Mannheim, Germany. IEEE Computer Society, 2010
7. Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda: All your contacts are belong to us: automated identity theft attacks on social networks. In: WWW 09: Proceedings of the 18th international conference on World wide web, New York, NY, USA, 2009. ACM
8. Facebook Press Room: Statistics, `http://www.facebook.com/press/info.php?statistics` (Accessed on June 24th, 2010)
9. PleaseRobMe, `http://www.PleaseRobMe.com`
10. BIK BITV Test, `http://www.bitvtest.de`
11. Eons, `http://www.Eons.com`
12. PatientsLikeMe, `http://www.PatientsLikeMe.com`
13. Dailystrength, `http://www.DailyStrength.org`
14. MedHelp - online discussion board on healthcare topics, `http://www.MedHelp.org`
15. Vu, Chambers, Garcia, Creekmur, Sulaitis, Nelson, Pierce, Proctor: How users read and comprehend privacy policies. In: Proceedings of the 2007 conference on Human interface, Berlin, Heidelberg, 2007. Springer-Verlag
16. Robert W. Proctor, Kim-Phuong L. Vu and M. Athar Ali: Usability of user agents for privacy-preference specification. In: Proceedings of the 2007 conference on Human interface, Berlin, Heidelberg, 2007. Springer-Verlag, ISBN 978-3-540-73353-9
17. Katherine Strater, Heather Richter Lipford: Strategies and struggles with privacy in an online social networking community. In: BCS-HCI 08: Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008, pages 111119, Swinton, UK, UK, 2008. British Computer Society
18. John A. Waterworth, Soledad Ballesteros, Christian Peter, Gerald Bieber, Andreas Kreiner, Andreas Wiratanaya, Lazaros Polymenakos, Sophia Wanche-Politis, Michele Capobianco, Igone Etxeberria, Louise Lundholm: Ageing in a Networked Society Social Inclusion and Mental Stimulation. In: Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, ACM ISBN 978-1-60558-409-6
19. Aaron Marcus: SeniorCHI: the geezers are coming! In: interactions, Volume 13, Issue 6 (November + December 2006), pages 48-49, ACM ISSN 1072-5520
20. Mary Applegate, Janice M. Morse: Personal privacy and interactional patterns in a nursing home. In: Journal of Aging Studies Volume 8, Issue 4, Winter 1994, Pages 413-434, Elsevier Inc.
21. Dr. Thilo Weichert: Datenschutzrechte der Patienten, `https://www.datenschutzzentrum.de/medizin/arztprax/dsrdpat1.htm`