Designing Privacy-Sensitive Healthcare Applications for the Home Domain

Carsten Röcker and Martina Ziefle
Human Technology Centre, RWTH Aachen University
Theaterplatz 14, 52056 Aachen, Germany
{roecker, ziefle}@humtec.rwth-aachen.de

ABSTRACT

Technology-enhanced homecare environments mark a big step towards increased quality of life for elderly and disabled people at home. While the potential benefits of smart healthcare solutions are undeniable, privacy-sensitive design concepts are necessary to guarantee their wide-spread adoption. This paper takes a closer look at privacy regulation mechanisms in everyday life and illustrates the importance of incorporating these intuitive human processes into the design of future homecare applications.

Author Keywords

Ambient Assisted Living, Smart Healthcare Applications, Intelligent Environments, Privacy.

ACM Classification Keywords

H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION

Ambient Assisted Living (AAL) environments mark a big step towards enhanced quality of life for elderly and disabled people at home. By reducing the need of caretakers, personal nursing services or the transfer to nursing homes, AAL environments can improve the daily life of elderly people and enable them to grow old at home (Hanak et al., 2007; Palen and Aaløkke, 2006). Maintaining independent as long as possible and not becoming a burden for others is widely accepted as the major contributing factor to quality of life in old age (see, e.g., Lindley et al., 2008 or Forlizzi et al. 2004).

While the potential benefits of technology-enhanced homecare environments are indisputable, privacy-sensitive design concepts are a crucial criteria for the acceptance of Ambient Assisted Living environments. This is circumstantiated by a variety of studies on different aspects of privacy in home environments. For example, in a survey by Privacy Rights Clearinghouse (2003) participants indicated that privacy protection was more important to them than any potential benefits provided by technologies found in Ambient Intelligence applications (Cook et al., 2009). Related studies also show that users are often not willing to take appropriate measures for protecting their privacy (Lahlou, 2008). A variety of authors including Chellappa and Sin (2005), Hann et al. (2002), Spiekermann et al. (2001) or Acquisti and Grossklags (2005) report findings indicating an obvious dichotomy between privacy attitudes and actual behavior. In order to gain a better understanding for this prevalent behavioral conflict, the following section takes a closer look at privacy regulation processes in real-life situations.

PRIVACY REGULATION IN EVERYDAY LIFE

Traditionally, privacy was regarded as a state of social withdrawal. In contrast to this widely accepted concept, Altman (1975) sees privacy as a boundary regulation process in which individuals optimize their accessibility along a spectrum of 'openness' and 'closedness' depending on their current context (Palen and Dourish, 2003). According to his Privacy Regulation Theory (Altman, 1975) privacy consisted of two processes, which regulate interaction with others: a dialectic process and a dynamic process. In a dialectic process, personal privacy is regulated depending on by our own expectations and experiences, and by those of others with whom we interact (Palen and Dourish, 2003). In a second dynamic process, privacy is continuously managed according to circumstances (Moncrieff et al., 2008). Hence, privacy is not only influenced by our own perceptions and those of others, but is also a continuous negotiation process depending on the current situation (Moncrieff et al., 2007).

In everyday life, people create and maintain personal privacy by understanding the privacy implications relevant to a situation and influencing them through a variety of social actions (Lederer et al., 2003a). The sum of these behavioral mechanisms and actions is referred to as 'privacy mechanisms' (Altman and Chemers, 1980). Altman (1975) classifies privacy mechanisms into four categories: (1) verbal behaviors: the use of the content and structure of what is being said, (2) non-verbal behaviors: the use of body language, like gestures or posture, (3) environmental mechanisms: the use of physical artifacts and features of an environment, like walls, doors, spatial proximity, timing, and (4) cultural mechanisms: the use of cultural practices and social customs (Neustaedter and Greenberg, 2003). Depending on the circumstances, individuals use a combination of different mechanisms to achieve a desired level of privacy, while one mechanism may substitute the other from situation to situation (Lehikoinen et al., 2008).

PRIVACY IN DIGITAL ENVIRONMENTS

In technology-enhanced environments social behavior will play a far more important role than in present technologies. As physical frontiers and sensual borderlines blur, common principles like – if I can see you, you can see me – no longer fit. This disintegration arise feelings of uneasiness, which might not only lead to the rejection of those systems, but even evoke fears. Those diffuse fears are often manifested in privacy and security concerns about new technologies. Several studies with existing technologies confirm these tendencies (see, e.g., Cole et al., 2001).

As explained above, privacy is a social space where personal development and regeneration happens. Technology-enhanced environments have to provide this space, and learn "how people manage accomplishments such as addressing, attending to and politely ignoring one another (Bellotti et al., 2002)". Hence, privacy should not become a matter of trust or mistrust. Experiences with existing systems showed, that most invasions of privacy are not intentional or malicious, rather designers failed to anticipate, how the system could be used, by whom, and how this might affect users (Adams, 2000). Therefore, it is the designer's task to build up confidence in technology and reduce privacy concerns and fears towards it. Especially in the early stages of technological development, decisions have to be made that have far-reaching consequences for the future costs of privacy protection. Only a timely and methodical approach allows getting on top of the multitude of privacy problems, and to develop assistive home environments that meet fundamental user needs.

TOWARDS PRIVACY-SENSITIVE ENVIRONMENTS

Privacy has long been identified as a critical factor in the design process of modern information and communication systems and a considerable amount of research has been conducted in the last decades (Lederer et al., 2004). Most early studies were addressing online and internet privacy (see, e.g., Hann et al., 2002; Taylor, 2003; Turow, 2003 or Cranor et al., 2000). With the emergence of location-aware ubiquitous computing applications, several authors started studying the willingness of users to share location information and their requirements regarding the protection of location data. For example, Barkhuus and Dey (2003) conducted several experiments exploring the acceptance of ubiquitous computing systems and found that around 30% of the participants would never use location-tracking applications due to their intrusive nature (Iqbal and Lim, 2008). A similar study on the willingness of users to share location data was conducted by Krumm (2009). Hong and Landay (2004) conducted a scenario-based study on context-aware applications in order to identify end-user requirements for such services. Further studies on location privacy have been conducted by Beckwith (2003), Cvrcek et al. (2006) or Danezis et al. (2005). In addition, interviews and surveys exploring more general aspects of privacy in context-aware systems were performed by Harper et al. (1992), Kaasinen (2003), Lederer et al. (2003b) or Hann et al. (2002).

In addition, several authors proposed mechanisms for protection privacy in digital environments. With respect to location privacy in sensor-enhanced environments, solutions were proposed by Ouyang et al. (2008), Boyer et al. (2006) or Fidaleo et al. (2004). There is also a considerable body of work on privacy-enhancing mechanisms for video-based communication systems. In an effort to help mitigate privacy concerns over video links, a variety of different techniques have been studied (Neustaedter and Greenberg, 2003). One of the most popular approaches is the usage of distortion filtration, an algorithmic reduction of the image fidelity, in order to hide sensitive details in the video images (Boyle, 2005). A number of different image blurring techniques, masking out sensitive areas in the video images, have been developed and tested by various authors (e.g., Coutaz et al., 1997; Zhao and Stasko, 1998; Boyle et al., 2000; Greenberg and Kuzuoka, 1999 or Neustaedter et al., 2003). Further concepts for privacy protection in ubiquitous computing applications were presented by Ackerman and Cranor (1999), Dourish and Redmiles (2002), and Hong et al. (2005).

On a conceptual level, current privacy protection mechanisms could be distinguished regarding different aspects: (1) protection of captured data vs. restricted capturing and (2) continuous protection vs. context-adapted protection. While most approaches aim at achieving privacy by implementing data protection mechanisms, so that personal data can only be accessed by authorized persons, other systems preserve privacy by restricting the amount of information being acquired and stored to the absolute minimum right from the beginning (Meyer and Rakotonirainy, 2003). Moncrieff et al. (2008) also distinguish between approaches where privacy protection mechanisms are implement by default (e.g., Senior et al., 2005) and applications providing privacy based on the environmental context of the user (e.g., Wickramasuriya et al., 2004). While the overall goal of supporting users in maintaining personal privacy is always the same, the underlying concept could largely effect the users' perceptions about the effectiveness of the general method. This in turn is likely to influence whether users trust and adapt a specific protection mechanisms or not.

CONCLUSIONS

While existing mechanisms for protecting user privacy provide valuable support functionalities, Cvrcek et al. (2006) argue that most users are not prepared to accept the overhead or cost, which current protection mechanisms require. This opinion is shared by a variety of authors. Like privacy regulation in real life, the implemented strategies should be lightweight and transparent (Neustaedter and Greenberg, 2003), requiring minimal additional effort from the user. In contrast, the involvement of technical systems complicates the privacy regulation process, as existing technical mechanisms do not adequately support known and intuitive human processes (Lederer et al., 2003a).

As illustrated in this paper, privacy has multiple functions and embraces diverse areas of life. Being a cluster of concepts, various aspects gather around the notion of privacy. All those aspects have to be reflected in order to create environments, which meet fundamental privacy standards. In this context, Palen and Dourish (2003) argue that even if surveillance and personal identity theft might be the most prominent and extensively studied concerns associated with ubiquitous computing systems, users mostly care about interpersonal privacy in the physical environment, like minimizing embarrassment, protecting territoriality or staying in control of their time.

In contrast to the majority of earlier research, which either focused on unauthorized access to digital information or addressed singular aspects of context-aware systems, it is important to take a much broader view when studying privacy in technology-enhanced spaces. Smart homecare environments have to be regarded as highly complex socio-technical systems and future research has to accommodate the fact that privacy violations can happen on multiple levels and in different contexts, both in the real and virtual world. In order to design trusted systems it is necessary to get a detailed understanding about the needs and wants of potential end users regarding privacy management in Ambient Assisted Living Environments. This does not only involve the acceptance of different regulation mechanisms, but also the appropriateness and usability of different approaches for everyday usage.

ACKNOWLEDGMENTS

This research was supported by the excellence initiative of the German federal and state governments.

REFERENCES

Ackerman, M.S., Cranor, L.F. and Reagle, J. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. Proc. ACM Conference on Electronic Commerce, ACM Press (1999), 1-8.

Acquisti, A. and Grossklags, J. Privacy and Rationality in Individual Decision Making. In IEEE Security and Privacy 3, 1 (2005) 26-33.

Adams, A. (2000) Multimedia Information Changes the Whole Privacy Ballgame. Proc. Conference on Computers, Freedom and Privacy, 25-32.

Altman, I. The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Brooks/Cole, Monterey, CA, USA (1975).

Altman, I. and Chemers, M. Culture and Environment. Wadsworth, Belmont, CA, USA (1980).

Barkuus, L. and Dey, A. Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns. Proc. Interact 2003, 709-712.

Beckwith, R. (2003). Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive 2, 2, 40-46.

Bellotti, V., Back, M., Edward, W.K., Grinter, R.E., Henderson, A. and Lopez, C. Making Sense of Sensing Systems: Five Questions for Designers and Researchers. Proc. CHI 2002, ACM Press (2002), 415-522.

Boyer, J. P., Tan, K. and Gunter, C. A. Privacy Sensitive Location Information Systems in Smart Buildings. Proc. SPC 2006, Springer (2006), 149-164.

Boyle, M. (2005) Privacy in Video Media Spaces. PhD Thesis, University of Calgary, Department of Computer Science, Calgary, Alberta, Canada.

Boyle, M., Edwards, C. and Greenberg, S. The Effects of Filtered Video on Awareness and Privacy. Proc. CSCW 2000, ACM Press (2000), 1-10.

Chellappa, R.K. and Sin, R. Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management 6, 2-3 (2005), 181-202.

Cole, J., Suman, M., Schramm, P., Lunn, L., Coget, J.-F., Firth, D., Fortier, D., Hanson, K., Jiang, Q., Singh, R., Yamauchi, Y. and Aquino, J.-S. The UCLA Internet Report: Surveying the Digital Future. UCLA Center for Communication Policy, Los Angeles, CA (2001).

Cook, D.J., Augusto, J.C. and Jakkula, V.R. Ambient Intelligence: Technologies, Applications, and Opportunities. Pervasive and Mobile Computing 5, 4 (2009), 277-298.

Coutaz, J., Crowley, J.L. and Bérard, F. Eigen-Space Coding as a Means to Support Privacy in Computer-Mediated Communication. In: Proc. Interact 1997, 532 -538.

Cranor, L., Reagle, J. and Ackerman, M.S. Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. In: I. Vogelsang, B. M. Compaine (Eds.): The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy. MIT Press, Cambridge, MA, USA (2000), 47-70.

Cvrcek, D., Kumpost, M., Matyas, V. and Danezis, G. A Study on The Value of Location Privacy. Proc. WPES 2006, ACM Press (2006), 109-118.

Danezis, G., Lewis, S. and Anderson, R. How Much is Location Privacy Worth? In: Proc. Workshop on the Economics of Information Security, Harvard University, CA, USA (2005).

Dourish, P. and Redmiles, D. An Approach for Usable Security Based on Event Monitoring and Information Visualization. Proc. NSPW 2002, ACM Press (2002), 75-81.

Fidaleo, D.A., Nguyen, H.-A. and Trivedi, M. The Networked Sensor Tapestry (NeST): A Privacy Enhanced Software Architecture for Interactive Analysis of Data in Video-Sensor Networks. Proc. VSSN 2004, ACM Press (2004), 46-53.

Forlizzi, J., DiSalvo, C. and Gemperle, F. Assistive Robotics and an Ecology of Elders Living Independently in Their Homes. Human-Computer Interaction 19, 1-2 (2004), 25-59.

Greenberg, S. and Kuzuoka, H. Using Digital but Physical Surrogates to Mediate Awareness - Communication and Privacy in Media Spaces. Personal Technologies 3, 4 (1999), 182-198.

Hanak, D., Szijarto, G. and Takacs, B. A Mobile Approach to Ambient Assisted Living. Proc. MCCSIS 2007, IADIS (2007).

Hann, I.-H., Hui, K.-L., Lee, T.S. and Png, I.P.L. The Value of Online Information Privacy: Evidence from the USA and Singapore. Proc. International Conference on Information Systems 2002.

Harper, R.H.R., Lamming, M.G. and Newman, W.H. Locating Systems at Work: Implications for the Development of Active Badge Applications. Interacting with Computers 4, 3 (1992), 343-363.

Hong, D., Yuam, M. and Shen, V.Y. Dynamic Privacy Management: A Plug-In Service for the Middleware in Pervasive Computing. Proc. MobileHCI 2005, ACM Press (2005). 1-8.

Hong, J.I. and Landay, J.A. An Architecture for Privacy-Sensitive Ubiquitous Computing. Proc. MobiSys 2004, ACM Press (2004), 177-189.

Iqbal, U.S. and Lim, S. A Survey on Users' Willingness-to-Pay for Privacy in Mobility Pricing Systems. International Journal of Liability and Scientific Enquiry 1, 3 (2008), 306-317.

Kaasinen, E. User Needs for Location-Aware Mobile Services. Personal and Ubiquitous Computing 7, 1 (2003), 70-79.

Krumm, J. A Survey of Computational Location Privacy. Personal and Ubiquitous Comp. 13, 6 (2009), 391-399.

Lahlou, S. Identity, Social Status, Privacy and Face-Keeping in Digital Society. Social Science Information 47, 3 (2008), 299-330.

Lederer, S., Hong, J.I., Dey, A.K. and Landay, J.A. Personal Privacy Through Understanding and Action: Five Pitfalls for Designers. Personal and Ubiquitous Computing 8, 6 (2004), 440-454.

Lederer, S. Mankoff, J. and Dey, A.K. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. Ext. Abstracts CHI 2003, ACM Press (2003b), 724-725.

Lederer, S., Hong, J.I., Dey, A.K. and Landay, J. A. Personal Privacy Through Understanding and Action: Five Pitfalls for Designers. Technical Report IRB-TR-03-035, Intel Research Berkeley (2003a).

Lehikoinen, J.T., Lehikoinen, J. and Huuskonen, P. Understanding Privacy Regulation in UbiComp Interactions. Personal and Ubiquitous Computing 12, 8 (2008), 543-553.

Lindley, S.E., Harper, R. and Sellen, A. Designing for Elders: Exploring the Complexity of Relationships in Later Life. Proc. HCI 2008, 77-86.

Meyer, S. and Rakotonirainy, A. A Survey of Research on Context-Aware Homes. Proc. Conferences in Research and Practice in Information Technology, Vol. 21, Australian Computer Society (2003), 159-168.

Moncrieff, S., Venkatesh, S. and West, G. Privacy and the Access of Information in a Smart House Environment. In: Proc. Multimedia 2007, ACM Press (2007), 671-680.

Moncrieff, S., Venkatesh, S. and West, G. Dynamic Privacy Assessment in a Smart House Environment Using Multi-Modal Sensing. ACM Transactions on Multimedia Computing, Communications, and Applications 5, 2 (2008), Article 10.

Neustaedter, C. and Greenberg, S. The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness. Proc. UbiComp 2003, 297-314.

Neustaedter, C., Greenberg, S. and Boyle, M. Balancing Privacy and Awareness for Telecommuters Using Blur Filtration. Report 2003-719-22, Department of Computer Science, University of Calgary (2003).

Ouyang, Y., Xu, Y., Le, Z., Chen, G. and Makedon, F. Providing Location Privacy in Assisted Living Environments. Proc. PETRA 2008.

Palen, L. and Aaløkke, S. Of Pill Boxes and Piano Benches: 'Home-Made' Methods for Managing Medication. Proc. CSCW 2006, ACM Press (2006), 79-88.

Palen, L. and Dourish, P. Unpacking 'Privacy' for a Networked World. Proc. CHI 2003, ACM Press (2003), 129-136.

Privacy Rights Clearinghouse. RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. Privacy Rights Clearinghouse, San Diego, CA (2003).

Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.-L., Ekin, A., Connell, J., Shu, C. F. and Lu, M. Enabling Video Privacy through Computer Vision. IEEE Security and Privacy 3, 3 (2005), 50-57.

Spiekermann, S., Grossklags, J. and Berendt, B. E-Privacy in Second Generation E-Commerce: Privacy Preferences Versus Actual Behavior. Proc. EC 2001, ACM Press (2001), 38-47.

Taylor, H. Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade it Off for Other Benefits. Harris Interactive Survey, Rochester, NY, USA (2003).

Turow, J. Americans and Online Privacy: The System is Broken. Technical Report, Annenberg Public Policy Center, University of Pennsylvania, Philadelphia, PA, USA (2003).

Wickramasuriya, J., Alhazzazi, M., Datt, M., Mehrotra, S. and Venkatasubramanian, N. Privacy-Protecting Data Collection in Media Spaces. In: Proc. Multimedia 2004, ACM Press (2004), 48-55.

Zhao, Q.A. and Stasko, J.T. Evaluating Image Filtering Based Techniques in Media Space Applications. Proc. CSCW 1998, ACM Press (1998), 11-18.