Aging, Privacy, and Home-Based Computing: Development of a Framework for Design

Kalpana Shankar , L. Jean Camp, , Kay H. Connelly, Lesa Huber

Indiana University
150 S Woodlawn Avenue
Bloomington, IN 47401, USA

Keywords

Pervasive computing; privacy; design; gerontechnology

Abstract

While the vast majority of information technologies are designed for younger audiences, recently more attention has been given to home-based applications that can help older adults "age in place". These designs focus on monitoring and providing support for elders while simultaneously providing caregivers the information needed to keep the elder safe. Relatively little attention has been given to the many ethical issues surrounding these types of pervasive technology. In this paper, we discuss the development of a privacy framework for design that we derived from the literature for the development of home-based computing for seniors. Using data from focus groups with over 60 elders, we address how the needs of elders, the perception of technology as a potential solution for aging in place, and the concept of privacy differ across the prototypes as well as between the researchers and the elders. We refine the framework to reflect the concerns and feedback of our research participants and then examine implications for the design of privacy-sensitive technologies for seniors.

Keywords: Computers and Society: Public Policy Issues: Computer-related health issues; Computers and Society: Public Policy Issues: Privacy**;** Computers and Society: Social Issues: Special needs/ elders; Computers and Society; Organizational Impacts: Deployment, usage experience

1 Introduction

Research on privacy from the security community has reasonably assumed there exists a demand for privacy, that privacy is an instrumental value, and that what actually constitutes privacy varies within the population and across contexts. Building upon this foundation, user-centered privacy mechanisms are built upon an assumption of individual privacy preferences. For example, the Platform for Privacy Preference (P3P) protocol enables server-side standards that can be easily and automatically interpreted and customized by the user and assume a single privacy rating of dimension [1, 2]. Other often-used approaches have used similar models to create typologies of orientations to privacy [3]. However, most of these approaches have not proved sufficient for predicting privacy concerns or privacy behavior [4,5,6], or distinguishing the very different

psychological elements of privacy elements: solitude, anonymity, reserve and isolation. Demographic variables such as age, gender, and education complicate privacy choices. As a result, there are numerous, often conflicting definitions of privacy. At its core privacy is a socially constructed value that differs significantly across environments and age cohorts of individuals. Yet knowing that this is true does not provide useful guidance to designers of information and communications technologies.

Our specific research domain is building privacy-aware ubiquitous computing for elders. There is a great deal of research and commercial interest in developing suitable applications to help older adults "age in place" [7, 8]. A confluence of factors suggests that this is an important and growing area: increased longevity, a shrinking pool of family caregivers, the advent of inexpensive monitoring technologies, and an increasingly burdened health care system. Such technologies can be empowering to elders and their families alike, but they also pose a risk of unnecessarily stripping the elders of privacy. The time to address these risks is at the design stage of new technology, if not before.

In this paper, we describe results of our research agenda through which we have been addressing the design at the intersection of aging, pervasive or ubiquitous computing, and privacy. In the next section we describe our rationale for this focus and our initial, literature-derived framework for privacy. In Section 3, we describe the prototypes we developed and purchased in order to instantiate this framework. In Section 4, we describe both the research design and analysis. The fifth section describes the results. The final section reconsiders our initial framework in light of the empirical findings and points to our current and future work in this arena.

2 Initial Privacy Framework and Related Work

As we noted, the term privacy has numerous definitions, drawn from many disciplines and practices. We limited our choices to those we anticipated would be particularly relevant to home-based computing (and could be instantiated through prototypes), most commonly discussed, and those that other researchers had emphasized in research similar to our own, then examined these through the lens of technologies that are currently being developed for use in the home. We began with privacy as **seclusion,** or "the right to be left alone" [9]. A constantly "on" monitoring system in the home, for example, would violate this construct if there were no location where a person could choose to be free from monitoring (e.g., if there were a visitor). However, those locations where people would most likely wish to be "left alone" (such as a bathroom) may be those where monitoring is most needed. Another common concept we employed is privacy as **autonomy**. Constitutional definitions of privacy encompass autonomy and its effects. Autonomy, or the right to self-determination, is violated if a person's activities are curtailed, or if the person perceives curtailment or fears it and thus does not engage in those activities. Home-based computing can violate privacy as autonomy if it creates a chilling effect, preventing elders from certain activities for fear of surveillance [10]. Privacy can also be perceived as **property**, in that it entails the right to determine the uses and dissemination of personal information [11]. The use of demographic information to enable price discrimination, for example, is a model of this dimension of privacy as pricing and property [12]. In pervasive computing environments, privacy is often constructed as a **spatial construct** where privacy involves establishing and respecting boundaries, both physical and virtual ones [13,14, 15, 16]. The fifth framing, that of privacy as a form of **data protection**, is where data generated are subject to consent to use and correction by the individual.

We operationalized this framework in two ways: as explicit design considerations in prototypes and as scenario development for focus group questions. The goal was to illustrate these framings of privacy both through artifact development (for elders' interaction and comments) and discussion (through extended open-ended focus group questions). In the next section, we describe the design of prototypes and selection of commercial technologies that would illustrate this framework

3. Prototypes

We selected six commercial technologies and prototypes that allowed us to explore a wide range of implementation issues, our selected privacy constructs, and potential for usefulness with respect to aging in the home. In this section, we discuss the selection criteria for the technologies, and describe the technologies we chose in more detail.

The first selection criterion we applied was the potential usefulness of the application for our target audience. Technology acceptance models and theories indicate that perceived usefulness is the primary factor in user acceptance [16, 17]; thus, it was important to select technologies that address the different needs of elders. When looking specifically at elders, the literature identifies four major domains in which technology could support independent, active aging [18]:

1. health monitoring and maintenance:
2. personal safety:
3. activities of daily living:
4. social well-being:

Our second selection criterion centered on data collection and informational privacy. Thus, we selected technologies that collect different data types (e.g., video, audio, financial), use the data in different ways, and thus facilitate more general discussion of technology use and privacy.

Our final selection criterion was aesthetics. An unattractive object or one with an intrusive or inappropriate form factor will not be easily accepted, no matter how useful it may be. Furthermore, an unattractive form factor might reduce the ability of the focus group participants to envision the object's usefulness in their own home. Thus, the devices we created needed to fit into the home of the average elder.

Every prototype had to address issues of data transparency. Since the integration of information technology is increasingly being embedded in everyday objects (one of the hallmarks of pervasive computing), it can lead to *invisible* data collection and use, a serious issue when addressing privacy concerns. Transparency, or at least the ability to be transparent, was a precondition in our choice of prototypes.

In order to cover these different areas of interest with a relatively small number of prototypes, we selected three off-the-shelf technologies and designed four specifically for this project. In the remainder of this section, we describe the four prototypes we developed in some detail, and list the off-the-shelf technologies. For each, we indicate how they fit into our selection criteria.

Ambient Plant: In addition to facilitating social well-being by keeping remote family members connected, the Ambient Plant can provide information about daily activities, depending on where a person places their plant in their home [19]. The prototype augments a flowerpot containing a fern with sensors and lights to facilitate awareness between remote family members. When a person is in the proximity of their plant, the remote pot conveys this activity by turning on its lights. For example, in our initial evaluation the adult child placed her plant on the desk in her home office, while the elder parents placed their plant in a sunroom next to their kitchen in which they eat their meals. When the daughter's pot lit up, she knew her parents were most likely having a meal; while the parents could tell when their daughter was working from home.

Mirror Motive: The Mirror Motive is a reminder and scheduling system embedded in a mirror on the wall. From across the room, the mirror is indistinguishable from a normal household mirror. When approached, a proximity sensor triggers the display to appear on the mirror. We integrated a number of scenarios, including displaying weather information, reminders (medical and social events) and invitations to social events. Interaction with the mirror is straightforward, with an elder acknowledging a reminder or accepting/declining an event or invitation by waving a hand in front of the appropriate choice.

Portal Monitor: The Portal Monitor addresses physical security by providing real-time digital photo alerts to a caregiver's cell phone whenever the doorbell rings or the front door is opened. The Portal Monitor consists of three cameras. One camera is inside facing the back of the closed door; one has a fisheye view out of door 5'5"

off the ground; and a third faces inward at the front of the closed door. The cameras are triggered either by the doorbell or by the door opening. Upon activation the Monitor's cameras take three pictures, two seconds apart, and send these via the cellular network to one or more cell phones selected by the elder.

Ambient Trust Cube: The Ambient Trust Cube, shown in Figure 3, is a frosted glass cube connected to a personal computer. When an individual accesses a particular website, the Cube provides a color indication of the likelihood that the website is malicious. Trustworthiness is determined by a combination of white lists maintained by trusted organizations and reputation built by the individual's history of interaction with the site. Effectively, the reputation system builds upon the observation that malicious sites have a short window of efficacy before they are discovered by anti-fraud, anti-phishing, or computer security analysts [20]. Thus a new site is considered untrustworthy unless otherwise specified on a white list while a site that has been repeatedly visited is considered trusted (again unless otherwise specified).

In addition to video cameras in each room, we also selected three off the shelf commercial devices. The **MD2** is an Internet-enabled medication dispenser. The dispenser has audio and visual notification, which continues until the elder presses a button that causes the medicine to be dispensed. If the elder does not press the button within a specified time, an alert can be sent to an informal caregiver and/or medical professional. **MindFit** is an off-the-shelf software application marketed to promote cognitive efficacy. The user plays various games and takes quizzes to maintain and improve mental functioning. MindFit data is sent to the company and auto-generated feedback is sent back to the user. Lastly, Wild Divine is a biofeedback application designed to be used to monitor and improve one's stress levels. Sensors are placed on the fingers, allowing the user to play a game by controlling his/her heart rate. In the table below, we summarize the Functionality, Usefulness, and Privacy Constructs represented by each application or device:

4 Research Design

As we noted earlier, the usability of the prototypes and commercial devices, while important, were of less immediate concern than their instantiation of the privacy framework and their potential for eliciting concerns of privacy, security, and other ethical considerations. We began with these open-ended research questions:

- Does the privacy framework we constructed hold for developing home-based ubiquitous computing?
- Does the privacy framework express privacy concerns for older adults?
- Are those concerns consistent across different prototypes, that is, do the concerns expressed about one prototype map to the concerns about another?

We expected that respondents would be most able to visualize the prototypes and understand their uses if they were displayed in a naturalistic setting. Therefore, we placed the prototypes in a real house in which the research participants could interact with the prototypes and ask questions of researchers. Each room had a single, functional prototype so that we could have multiple older adults interacting with different prototypes simultaneously, without distracting each other. Participants (n=65) in the focus groups ranged in age from 60 through 85. All were mobile, healthy, and cognitively high-functioning. Most were residents of a local retirement facility and most lived independently in cottage-style housing, but could take advantage of the central dining facilities and social activities. A preliminary anonymous survey was administered to each member of the group. From this survey, we learned that all of the seniors were familiar with at least some form of information technology (computers, cell phones, etc). A small minority of the group used a medical alert bracelet or other personal safety monitoring device; none had experience with any other monitoring or other home-based technologies.

We split larger groups of participants into smaller groups of two to four. In these smaller groups, the participants rotated through each room in the house where they were introduced to the prototype by a researcher, allowed to ask questions and interact with the prototype. The conversations with the researchers were video and audio taped for later transcription. After approximately ten minutes, they moved to the next prototype. When

the participants had seen all prototypes, we brought the whole group together to ask more explicit questions about their privacy concerns and presented them with scenarios to test the privacy framework.

With this format, we conducted several pre-tests in which we brought in three groups of four to six seniors at a time, aged 65 to 80. We used the results from the pre-test groups to refine the focus group questions, and then brought in four separate groups of 9-20 participants each. Because these groups were so large, at the end of rotating through the prototypes participants were divided into two groups for the focus group portion of the study instead of one large group.

Audio interviews of individual sessions with prototypes and concluding focus groups were transcribed. Transcripts were coded for themes that either supported or negated dimensions of the initial framework, as well as other themes related to privacy, usefulness, and functionality as they reflected our initial questions. We mapped new open codes to the existing framework if applicable to refine our initial framework.

4 Results

4.1 Reactions to Prototypes

As we had anticipated, health monitoring and physical security (i.e., how the devices could be potentially useful in those arenas) were primary concerns of older adults. Prototypes that addressed ADLs and social well-being received mixed reactions. While participants often had specific suggestions for improvements, medical reminders and the cognitive and stress reductions games were almost universally liked. Somewhat surprisingly, participants were interested in being able to compare their performance to their peers, and thus were willing to have their data aggregated with a larger group. For these prototypes, they had no concerns about where the data were stored or data sharing.

Participants reacted positively to the prototypes addressing physical security, and indeed tried to appropriate some of the other technologies to enhance personal safety. For example, the Presence Clock and Ambient Plant were designed to give subtle indications of ADLs, depending upon where they were placed in the home. While participants did not object to this use, they would much rather use the technology to detect an emergency, such as a fall. They frequently noted that the Ambient Plant and Presence Clock could be used to detect if someone had not moved for an extended period of time, and thus had perhaps fallen and could not get help.

The Ambient Plant, Presence Clock and Mirror Motive all provided participants opportunities for enhanced connection with family members and others in the community. These technologies were not perceived to be as useful as we had originally expected. Almost all participants lived in some form of community, either with a spouse or in a retirement community. Respondents told us they had little need for technology-mediated social connections when planned activities, central socializing facilities, and in-person visits and phone calls provided enough socialization for both pleasure and safety. These findings, however, may not be generalizeable to the 33% of individuals over 65 who live alone [21].

The Ambient Plant and the Presence Clock are bidirectional. That is, not only can the informal caregiver see the activity levels of their loved one, the older adult can see the activity levels of the informal caregiver. We used these prototypes to explore if the bidirectionality made the technology was more acceptable to participants. This feature provoked mixed reactions. While some participants enjoyed the reciprocal nature of these prototypes that could give them insights into their children's lives, several were uncomfortable with asking their children to permit this and felt that they might intrude. When probed further, they admitted that while they liked the idea, they would not ask their children to use it. This suggests that there is a delicate balance of power and negotiation that must be navigated to make these prototypes useful.

4.2 Personal Data and Privacy

We initially chose our prototypes to explore different types of data being collected, with an emphasis on contrasting visible and invisible data collection. While our results clearly indicate that some older adults are more willing to allow some types of data to be collected than others, we found that our participants' understanding of what is being collected was often incorrect. Particularly problematic were prototypes that were embedded into everyday objects (such as the Mirror Motive), and in the affordances participants naturally attributed to a particular prototype. In this subsection, we describe both the results with respect to types of data, and how incorrect perceptions influenced the participants' concepts of privacy.

However, conceptualizing privacy as data protection only makes sense when one knows that data are being collected. Our results suggest that the concept of "data" as commonly articulated is too vague to communicate concrete impressions of what is at stake. None of the prototypes explicitly displayed the digital trail left by their use.

The Mirror Motive illustrates this lack of data transparency. Since the Mirror does not make explicit what data is being collected or how it is being used, participants did not express any concerns that this information was being stored, and possibly shared with others. However, it was clear to the participants that the MD2, the medication dispenser) may transmit compliance information to a medical provider, as a major function of the MD2 was to notify someone if a medication was missed. But even though the Mirror Motive was collecting (and possibly sharing) the same information, it was under the pretence of a *reminder*, not a *dispenser*. The participants did not understand that the same data could be collected and used even though the first-order purpose of the systems was different. In their minds, even though the Mirror Motive was obtaining information for the outside world (e.g., an invitation to go to their grandson's soccer game), it was physically located in its entirety in their living room, and thus not sharing data with the outside world.

It would be relatively straightforward to create a digital trail and demonstrate it within the prototype (e.g., show when data is being shared with other). We are now exploring how to incorporate data transparency in existing and new prototypes [22].

There is a long-standing argument for the importance of location privacy and the importance of spatial models of privacy. Our interviews and prototypes yielded a very different result: it is the activity and not the location that is critical. The most often used locations are sensitive because of their indicators of potentially sensitive behaviors. Bedrooms are perceived as sensitive spaces because of the likelihood of sex and the vulnerability of sleep. Bathrooms are sensitive because of the privacy of personal toilet. This aligns well with concepts of contextual integrity that has been evaluated in terms of computer security [23, 24].

This finding is more generalizable for design than privacy because it identifies that the same space may be one where individuals desire active surveillance (e.g., not falling the bathroom, being safe in the park at night) or would avoid surveillance (e.g., no photographs on the toilet, not being identified during a political protest in the park)[25]. This is an important distinction to make with respect to the placement of technology and data gathering: an older adult who is concerned about physical safety might very well be willing to accept monitoring technologies in spaces others might consider sensitive, because the risk of falling in such a space (such as a bathroom) is greater for that person.

In terms of technical implications, this strongly argues that any system should integrate subject control and tuning. In no case did we find that a single privacy setting was ideal. Even with very simple low-granularity prototypes in public spaces there was a strong desire to be able to temporarily shut down the technology in some cases. In other cases, the desire was to increase the amount of data in times of perceived crisis. Technology that would be turned off during a party would be turned up after all the guests had departed for the evening.

4.3 Data Recipient

Some privacy theorists have critiqued the neat dichotomy of public/private that characterizes much of the discourse on privacy [23, 24]. Although home-based computing seems to be the *sine qua non* of private space, data flows across boundaries of walls, networks, and devices challenges that characterization. Simply put, home-based ubiquitous computing generates data about people that can then be seen, commented upon, and re-used by others. Personal data are not neutral. Focus group participants were sensitive to how data could be used and by whom, even when they were not clear on what data was being generated by the prototypes they saw. This suggests that simple role-based access controls are not sufficient (e.g., "my children can access the system"). For example, respondents were often comfortable with one particular adult child "monitoring" data flows, but not another child, because that second child was a "worrier". Commercial uses of data (for targeted advertising, for example) were uniformly frowned upon, but academic research was considered acceptable, assuming data were aggregated and de-identified. These findings are not surprising if one accepts that all new technology has the potential to mediate and shape relations among individuals, institutions, and organizations. We exhort our colleagues as they proceed in this research space to reflect further on the specifics of power and mediation in home-based ubiquitous computing.

5 Reconsidering Our Framework

In our initial framework, we drew upon the existing literature and research to identify and operationalize key privacy metaphors for home-based computing and aging: autonomy, seclusion, data protection, protected space, and property. This framework was useful in framing initial design and testing, but as our results suggest, proved to be less effective at predicting the kinds of choices, decisions, and tradeoffs that older adults were willing to make. Our research challenged this framework because the initial framework focused closely on definitions of privacy but did not fully integrate how privacy would be determined. The other factors that we identified – usefulness of the technology, human relationships, and the nature and process of aging itself – acted in concert to contextualize privacy. In our modified framework, we interrogated our initial constructs to more fully reflect and integrate these other factors. In this section, we discuss this modified framework and an example of how we instantiated it.

Our results confirmed that the **usefulness** played a significant role in determining how individuals thought of privacy. The more useful the participants perceived a particular device or prototype to be with respect to their own lives, the more willing they were to accept wide variance in data transparency and collection and physical location of the prototype. Similarly, while **data granularity** played a role in the comfort levels of participants, it was not the only factor. For example, many participants expressed discomfort with the Ambient Plant and Presence Clock collecting and recording physical proximity. Yet these same participants were often quite happy with the Portal Monitor, which collected still photographs of the entryway. This appears to be because the cameras are pointed at a particular space (i.e., the door), and are being used for a particular, and very pertinent, reason (i.e., security). When queried about cameras in other parts of the home, participants were much less accepting. Indeed, discussion of video was often equated with feelings of imprisonment and "Big Brother". This in turn suggested that **spatial privacy** turned out to be less important than **activity sensitivity**. Lastly, a factor that was almost entirely elided in the initial framework was **data recipient.** While we acknowledged the importance of general relationships in assessing whether participants would be willing to share their data (for example, participants were more comfortable sharing data with researchers than marketers), the specificity of who would be allowed to see data was important; i.e., one daughter and not another. *Where* an element of technology is located in the home; *what* data are compiled; *how* to edit or correct the data; and *who* has access are core concerns for every older adult. However, rather than building on the abstract notion of data, our framework is now grounded in very specific activity constructs using well-defined data types. The final

construct in our original framework, data as property, was mostly foreign to our participants, even though that is the legal reality in which they live. One could argue usefulness is grounded in data as property. But while the concept is echoed in economic studies of utility of technologies versus willing to provide information, the elders themselves found it inapplicable. Participants often could not imagine *why* anyone would be interested in their data, so could not understand the implications of someone other than themselves owning data about them. As such, we are removing the notion of data as property from our framework.

We are still in the process of testing this redesigned framework empirically, but did derive at least one specific recommendation: greater transparency can be achieved through user empowerment to control the devices. We suggest that can be achieved through the implementation of three settings in the next generation of prototypes: turn on, turn off and pause. While the first two have long been common practice, the third is more of a broadly applicable innovation and potentially controversial

1) On: full functionality and data is transmitted

2) Off: the older adult can turn off the device and others are notified that it is off.

3) Pause: the device is off but the data recipient is not made aware the device is on.

One of the more critical elements of both was the ability to stop data collection without any announcement or visibility that it has stopped to anyone but the older adult. With more than one prototype, deceit in the form of technical inaccuracy was desired when questions of information sharing arose in our focus groups with older adults. They asked if there was a way to turn off the technology without the data recipient being aware that the technology was turned off. This can be problematic with technologies like the Presence Clock, where being off will be interpreted as inactivity. This could also be a safety hazard (one way around this problem was to have the device automatically turn itself back on). Yet with in-home technologies, the requirement for always-accurate data in the home creates a potential conflict with privacy. We are in the process of evaluating how such a "Pause Function" could work without abrogating safety and its use and reception by older adults and their loved ones.

6 Conclusions

The demographics of wealth, social isolation and changes in health and differences in cognitive function argue that older adults should be well-represented online and more generally, in the development of new information technologies. However, this demographic tend to be disproportionately underrepresented, not only in those applications consciously targeting the young (e.g., gaming) but also in the arenas of social networking and e-commerce. While the vast majority of technologies are designed for younger audiences, recently more attention has been given to technologies which can help older adults "age in place". These designs focus on monitoring and providing support for older adults while simultaneously providing caregivers the information needed to keep older loved ones safe. Relatively little attention has been given to the ethical issues surrounding these types of pervasive technology. Specifically, privacy is dismissed as a privilege of youth and health, as the alternative to privacy-invading technologies may be the loss of personal autonomy and agency.

The ETHOS project began with the proposition that the choice between digital and physical autonomy is a false choice. By definition, in-home technologies are introduced while the older adult is still living independently. In addition, the technology is presented in its entirety, with potentially privacy-influencing design choices embedded without the participant's examination. As such, it is essential to acknowledge the range of ethical considerations inherent in this context and design technologies that are sensitive to the values of the older adults, including privacy.

In this paper, we describe our initial theoretical framework of privacy, the development of prototypes to test that framework, and the results of a series of focus groups to better understand older adults' privacy concerns

with home-based technologies. We conclude with changes in our framework and illustrate how this revised framework can be instantiated in home-based ubiquitous computing.

There is strong evidence to suggest that integrating information technologies into people's daily lives can significantly enhance their quality of life. However, such integration requires that technologies be designed with human agency in mind. That theme is one of the key findings of our research with older adults, expressed by them as the belief that they wish to be on the active user side of the digital divide and not simply subjects of pervasive monitoring technologies. This desire to be an active user and not a passive subject of home-based technology expresses a larger theme: that overcoming the digital divide among older adults requires deep consideration of the ways in which technology mediates, influences, and is shaped by *human* relationships.

Acknowledgments. This work was funded by NSF grant #0705676. We wish to thank the anonymous reviewers who gave us such extensive and useful feedback. We also wish to thank Dr. Kelly Caine, William Hazlewood, Zach Zimmerman, Mary Boutain, Oliver McGraw, and the other students of the ETHOS lab for their hard work as well as the numerous participants who were part of the study.

References

[1] L.F. Cranor, *Web Privacy with P3P*. O'Reilly, 2002.
[2] H. Hochheiser, "The platform for privacy preference as a social protocol: An examination within the U.S. policy context", *ACM Transactions on Internet Technology (TOIT)*, vol.2 no.4, pp. 276-306, Nov. 2002.
[3] A. Westin, "Consumer privacy and survey research", 2003, http://www.harrisinteractive.com/advantages/pubs/DNC_AlanWestinConsumePrivacyandSurveyResearch.pdf.
[4] J. King and C. J. Hoofnagle, "Californians' attitudes towards privacy of location data", *TPRC 2008*, Arlington, VA.
[5] K.H., Connelly, A. Khalil, Y. Liu, "Do I do what I say?: Observed versus stated privacy preferences", *Proceedings of the Eleventh IFIP TC13 International Conference on Human-Computer Interaction (INTERACT),* Rio de Janeiro, Brazil, September 2007, pp. 620-623.
[6] H. Bouma. "Technology for a purpose," *Proceedings from Gerontechnology*, Pisa, Italy, 2008.
[7] O.A., Blanson Henkemans, K.E. Caine, W.A. Rogers, A.D. Fisk, M.A. Neerinex, and B. de Ruyter, 2007. "Medical monitoring for independent living: user-centered design of smart home technologies for older adults," In *Proceedings of the Med-e-Tel Conference for eHealth, Telemedicine and Health Information and Communication Technologies*, Luxembourg City, Luxembourg, April 18-20, 2007.
[8] S. Warren and L. Brandeis, "The right to privacy," *Harvard Law Review,* vol. 4, pp. 193-220, 1890.
[9] J. E. Cohen, "A right to right to read anonymously: A closer look at copyright management in cyberspace," *Connecticut Law Review* vol. 28, no.4, pp. 981-1039, Summer 1996.
[10] P. Mell, "Seeking shade in a land of perpetual sunlight: privacy as property in the electronic wilderness," *Berkeley Technology Law Journal*, vol. 11, pp. 11-92, 1996.
[11] A. Odlyzko, "Privacy and price discrimination" in *Economics of Information Security* (eds. Camp & Lewis) Kluwer Academic Press, pp. 187-21, 2004.
[12] E. J. Bloustein, "Privacy as an aspect of human dignity: an answer to Dean Prosser," *New York University Law Review*, pp. 962-970, 1968.
[13] M. Langheinrich. "Privacy invasions in ubiquitous computing", *Ubicomp* 2002, Goteborg, Sweden, September 29-October 1, 2002.
[14] X. Jiang. "Safeguard privacy in ubiquitous computing with decentralized information spaces." *4th International Conference on Ubiquitous Computing,* 2002.
[15] S. Shapiro. "Places and space: The historical interaction of technology, home, and privacy, " *The Information Society*, vol. 14, no.4, pp. 275-284, 1998.
[16] B. Szajna, "Empirical evaluation of the revised technology acceptance model," *Management Science*, vol. 42, no. 1, pp. 85-92, 1996.
[17] S. Beach, R. Schulz, W. Bruin, J. Downs, D. Musa, and J. Matthew. "Disability, age, and information privacy attitudes and quality of life technology applications: results from a national Web survey," *ACM Transactions on Accessible Computing*, vol. 2, no. 1, May 2009.
[18] M. Alwan, D. Wiley, and J. Nobel. "State of technology in aging services," Center for Aging Services Technologies, Tech. Rep., Nov. 2007.
[19] W. Odom, H. Jung, W. R. Hazlewood, (2010, accepted). "Reflective inquires: a multi-dimensional approach to designing for domestic elderly life," In Proceedings of Design and Emotion. D&E '10, in press.
[20] A. Tsow, C. Viecco, and L.J. Camp, "Privacy-aware architecture for sharing Web histories," *IBM Systems Journal*, accepted, 2008.

[21] Administration on Aging: U.S. Department of Health and Human Services. “A profile of older Americans”, 2008. http://www.aoa.gov/AoARoot/Aging_Statistics/Profile/2008/docs/2008profile.pdf
[22] K. E. Caine, C. Y. Zimmerman, Z. Schall-Zimmerman, W. R. Hazlewood, A. C. Sulgrove, L. J. Camp, K. H. Connelly, L.M. Huber and K. Shankar, “DigiSwitch: design and evaluation of a device for older adults to preserve privacy while monitoring health at home”, *ACM International Conference on Health Informatics*, in press.
[23] H. Nissenbaum. “Privacy as contextual integrity.” *Washington Law Review*, vol. 79, no. 1, pp. 101-158, 2004.
[24] E. Felton, H. Nissenbaum, and B. Friedman. “Computer security: Competing concepts.” *The 30th Research Conference on Communication, Information and Internet Policy*, Arlington VA, September 2002.
[25] L. Little, P. Briggs, & L. Coventry “Public space systems: Designing for privacy,” *International Journal of Human Computer Studies*, vol. 63, no. 1-2, pp. 254-268, July 2005.

Author Bios

Kalpana Shankar is an Assistant Professor at the School of Informatics and Computing, Indiana University-Bloomington. Her research interests include scientific recordkeeping and data management practice the uses of pervasive computing in shaping social relationships. Starting in July 2011, she will be a lecturer in the School of Information and Library Science at University College Dublin. She received her Ph.D. in library and information science from the University of California, Los Angeles. She can be reached at shankark@indiana.edu or Kalpana.shankar@gmail.com or 901 E 10th Street, Rm 303, Bloomington IN 474703.

L. Jean Camp is an Associate Professor at the School of Informatics and Computing, Indiana University-Bloomington. Her research focuses on the intersection of social, economic and technical trust. She received her doctorate from Carnegie Mellon University in Engineering and Public Policy. She can be reached at ljcamp@indiana.edu or 901 E 10th Street, Rm 200, Bloomington IN 474703.

Kay Connelly is an Associate Professor in the School of Informatics and Computing at Indiana University-Bloomington. She is the Senior Associate Director of IU's Center for Applied Cybersecurity Research. Her research focuses on user acceptance of ubiquitous and mobile computing and health and wellness applications to empower both the ill and the healthy to manage and improve their own health and make healthy choices. She received her Ph.D. in computer science from the University of Illinois, Urbana-Champaign. She can be reached at Connelly@cs.indiana.edu or Informatics East Rm. 260, 901 E. 10th Street, Bloomington, IN 47408.

Lesa Huber is a Clinical Assistant Professor in the Applied Health Science Department, School of Health, Education, and Physical Recreation (HPER), at Indiana University-Bloomington. Her research interests include gerontology and geriatric education for health care professionals, physical activity and aging, creativity and aging, gerotechnology, and pedagogical strategies in distributed education. She received her Ph.D. in gerontology from the University of Lincoln-Nebraska. She can be reached at lehuber@indiana.edu or Smith Research Center, Room 197, Bloomington, IN 47405.