

Beyond Consent: User Defined Privacy in Ubicomp

L Jean Camp, Kay Connelly, Lesa Huber, and Kalpana Shankar

Demographic changes, longer life-spans, war, and advances in medical care which make previously fatal injuries or birth defects into manageable lifelong disabilities can be predicted to increase the need for home health care. The demand for home health care will be increased by social changes, in particular, the movement towards the mainstreaming of and community living for the chronically ill and disabled. Cost containment policies by insurers and hospitals have also contributed in that these policies lead to earlier discharge of chronically ill patients into the care of their families.

Ubiquitous computing, or ubicomp, holds promise for the development of easy-to-use technologies that enhance the ability of caregivers to monitor those in their care, but most extant technologies have not been developed in a socially-aware, privacy-sensitive context. More formal development of privacy-sensitive ubicomp design can enable nurturing rather than controlling ubicomp for independent living for the elderly and disabled.

Ubicomp integrates technology into our everyday environments. Ubicomp fundamentally alters privacy by creating continuous detailed data flows. The privacy challenge is particularly acute in the case of home-based health care where vulnerable populations risk enforced technological intimacy. The promise of ubicomp is also particularly great in the area of home-based ubicomp with the aging of the population. The combination of a vulnerable population, embedded computing, and inadequate privacy regimes may lead to a digital perfect storm.

Such an environment can truly result is a system that is too much computer-based nurturing for the subject, with nurturing broadly conceived as including protection. In fact, ubicomp in the home has the ability to lead us to an Orwellian society where people can no longer detect when they are interacting with the network and creating data records. Currently, there is no accepted methodology for creating respectful, nurturing home-based ubicomp.

Privacy in ubicomp for home-based elder care currently requires elders who can articulate specific technical privacy design choices, and designers who bring a profound understanding of privacy to the implementations of these specifications. Neither of these is likely. There is no single answer for the challenge of designing for privacy. Privacy is a socially constructed value that differs significantly across individuals.

Value-sensitive design has the potential to influence privacy by respecting the individual elder's conception of privacy. This is a challenge because value-sensitive design must be predicated upon a shared concept of the particular value under consideration.

If invited to the *Nurturing Technologies in the Domestic Environment Workshop*, we would begin with an introduction to value-sensitive design and a high-level overview of the competing concepts of privacy. We will critique each privacy construct with respect to home-based health care. We also hope to initiate a shared critique of privacy as constructed in home-based ubicomp systems, as indeed "too nurturing" for the elder concerned.

The Perfect Privacy Storm

As the numbers of elders increase, so will the need for health care. Home-based health care takes on increased importance as a major part of the US health care system with demographic aging. The US Government Accountability Office estimates that informal care (e.g. visits, chores, reminders, help with medicines, errands) accounts for more than 85% of all elder care. The amount of informal care given to elders is likely to increase as the baby-boom generation starts to use, and threatens to overwhelm, current formal health care systems. Indeed, the number of people over the age of 65 in the US is projected to double in the year 2030 to over 69 million, an increase from 8% to 22% of the US population.

Loss of privacy and detailed data surveillance are not inherent requirements for ubicomp. For example, consider a pressure sensor. What elder home health issues can be aided by such a sensor (e.g. identifying falls)? What filters are available that de-identify individuals (e.g. removing detailed gait information), count events (e.g. mild balance loss) without detailed recording, and obscure exact timestamps with time periods? What questions will enable the elder to analyze the pressure sensor, filters and application, in terms of his or her own home? To begin to answer these questions, we examine existing privacy paradigms, which include autonomy, seclusion and property.

The concept of privacy as autonomy brings forward the right to act without surveillance. If seclusion is the right to choose not to participate, autonomy demands participation without identification. Yet autonomy is often seen as implying protection of other data that could be embedded; for example, even a combination of blurred timestamps with gait-identifying pressure sensors could indicate sexual orientation in a fully active house. Obtaining correct individual perspectives on autonomy is a unique research challenge, as to ask, “What exactly is it you do not want us to learn?” is inane in any case, and is a particular oxymoron in privacy research.

The paradigm of privacy as seclusion illuminates the right to be left alone, leading to the questions: Does the elder want to be able to turn the technology off, or have it always on? Should someone (i.e. an informal caregiver) be notified if it is off? For example, gait identification in the home may be something that comforts the elder in the evening by identifying ‘thumps in the night’ as either caregiver or cat, but not an element which is desirable during more social daylight hours. The higher level of data might (not) be shared in the evening depending upon the individual elder’s desire to be left alone versus the subject’s sense of continuous ubicomp surveillance.

The privacy as property paradigm brings forward not only the alienable nature of data but the idea of the right to exclude. Exclusion is also the core of the spatial metaphor. Spatial questions can serve to bring autonomy to the fore by assisting users in defining sensitive or personal spaces. For example, an elder may not want tracking in and out of his bedroom. The framework as a whole must embed the understanding that removing the data from only the bedroom would be meaningless if the person disappeared off the house map into the bedroom only to reappear in the hall a specified time later. Thus the questions would be translated to indicate rough spatial filtering – in and out of the home only or better or worse balance in a given time period. Spatial questions can also assist in defining data boundaries.

Some elements of data protection bring rise to questions that address both privacy and ease of use: Will an elder want to review and interact with the data? Do they prefer visible ubicomp or embedded (invisible) designs? Should the elder know whenever a caregiver “drops in” or checks the data? Should the ubicomp monitoring system “reach out” to the caregiver for periodic checks? Does the elder want to actively manage his or her own data boundaries, or allow them to be highly permeable at all times? If desired, to whom should the data boundaries be opened? This brings back the details of property-like exclusion. The emphasis on visibility of data protection may not be appropriate for livable home-based ubicomp as people may tire of the conscious daily interactions.

Consider the case of medication adherence, which can indicate cognitive well-being. Failure to adhere to guidelines for taking medications can result in personal, emotional, and financial harm to elders and their caregivers. In an invisible design, sensors placed where medicine is kept and taken can detect if a person does not follow all of the instructions, takes the incorrect dosage, and takes doses at the wrong time or in the wrong combination. In a visible design, users can indicate that they have taken medication, e.g., by pressing buttons.

What is user-centered privacy and how does it relate to larger social/demographic changes in society? How should we elicit and design for individual needs for privacy and embed them in the tools and systems we design? How do we evaluate those tools for their privacy-enhancing potential and capabilities? How do we describe and present data to caregivers, participants, and others in a way that enhances privacy, minimizes confusion, and maximizes utility?

Our Response

Nurturing rather than surveillance ubicomp can be constructed if *the subject defines privacy*. At Indiana University, we are beginning to construct mechanisms for subject-defined privacy in ubicomp. Our approach is to build a privacy framework that is embedded into three components of a framework. For our work, a framework is distinguished from guidelines in that rather than providing specific answers, the framework assists in asking the right questions and provides different perspectives on the possible answers. A framework is distinguished from a paradigm in that the framework will incorporate distinct paradigms.

The first component is a participant tool for eliciting individual elder privacy concerns. The second is a tool that ubicomp designers can use to translate elder concerns into technical choices. The third is a privacy-enhancing code library for ubicomp sensors.

Our approach to nurturing design of ubicomp is based on constructing **a theoretical framework** of the privacy concerns of elders. The framework will inform the development of **a participant tool** to assist individuals (in this case, elders and their loved ones) in articulating their privacy concerns about home-based

ubicomputing. This framework interfaces with a **designer tool** which guides designers through a value-sensitive design process, translating the elder's concerns to resulting in a more acceptable design. The tool is built upon a **sensor library** that enables effective designs through a characterization of sensors based on specification of data provided by the sensors and a set of privacy enhancing technologies that are useful for each sensor (e.g. data filters). The following paragraphs describe these components.

Participant Evaluation Tool

The participant evaluation tool will enable individuals to express their own privacy concerns by participating in an interaction designed to function as a virtual interview. The participant evaluation tool will present design choices that the participants and caregivers can evaluate in terms of privacy preferences without technical knowledge. The personal conceptualization of privacy may differ between households or even individuals. Details of loss in compressed data or algorithms for providing limited quality of video are not likely to be useful to non-technical individuals, yet questions about specificity of information in different locations may be quite useful. The construction of the framework will focus explicitly on translations of those dimensions that can be addressed by design: exact data versus ranges, tracking versus interrupt generation, visible versus integrated technology, total count of events versus details on each event, etc.

The model of the participant evaluation software will be Software Development Impact Statements (SoDIS) which integrates ethics (as defined by the ACM Code of Ethics) into a decision-support and design-support framework. Designing the participant evaluation tool will require parsing the privacy perspectives into the theoretical concepts of privacy described above, translating those concepts into design implications, and then using additional interviews to iteratively increase the parsing itself was correct.

Designer Tool

The designer tool will present technical choices to the designer without requiring the designer to have a deep understanding of privacy. The tool provides notifications of potential privacy risks and questions to explore them, which will be obtained from the qualitative research on participants and the larger privacy literature. For example, upon selecting a location sensor, the framework might remind the designer that this is for home-based systems and thus the people are identifiable. It may generate location-specific questions: *Will this be on a medication bottle?* and if the answer is yes, a reminder *Medication data consumption should be kept in a time range of at 24 hours.* Some questions will be evocative, to assist the designer in taking basic data protection into account: *Who can access this information? What is its purpose? How long will it be kept?* Other questions may emerge from the privacy concerns of care-givers, e.g., *If frightened, can the subject use the system to make sure no one else is in the house? Can anyone determine how many people are in the house from observation of wireless output of the location sensors?* It will generate participant-specific warnings: *Do not track movements around the house; indicate medicine events only by time period.* The tool explicitly addresses the role of the participant in privacy-sensitive design, which recognizes ubicomp as a socio-technical system, by integrating concerns in the technical system. When examining the privacy implications of sensors in the complementary toolkit, it is important to include questions and guidelines to assist ubicomp designers to select the appropriate level of exclusivity in defining virtual boundaries. Integrating privacy (conceptualized as seclusion, autonomy, property, or spatial) into the design space can enable more effective privacy enhancing design and selection of the most appropriate privacy enhancing technologies (PETS).

The designer tool is tightly coupled with the sensor library (described below). The sensor library allows us to integrate basic concepts of privacy in terms of data protection into the toolkit. The sensor library describes the options for privacy-aware design in terms of data granularity, temporal data, and data aggregation that are specific for each sensor. Sensors are well-defined technical artifacts that produce well-specified types of data (e.g., location, movement, temperature, images, or audio). Because the data types are specified, the questions in the designer tool can be well targeted, for example, on data availability and specificity. As our research target is home health care, the designer tool can serve to remind developers that the data will have a high degree of specificity, so that theoretical mechanisms for ensuring anonymity in network data may not apply. As technologists make increasingly specific design choices, increasingly specific concerns are identified and specific privacy enhancing technologies can be suggested.

Privacy-Sensitive Sensor Library

Current home-sensor systems used to assist independent living in elder populations often collect as much information as possible and perform any data filtering at the application layer. Because of the sensitive nature of the data and the limited security expertise of most of the population, privacy is an ongoing consideration. One way for designers to address privacy is to select appropriate filtering that can be done before the data are stored, thereby protecting detailed information by simply not storing the data.

The capabilities of the library are a critical element of the toolkit. The toolkit includes the interfaces to elicit possible privacy issues for the technologists, and assist them in privacy-sensitive design. The designer tool alone, with no library, might function only as a questionnaire for high-level design decisions. With the library, the designer tool can enhance design at a detailed level.

The library simplifies the design of value-sensitive ubicomp by providing an easy to use API for the designer to select data specificity without being forced to program each choice by hand. For example, if the designer tool indicates that an appropriate design choice would be storing only a time range, the sensor library will provide a simple implementation of that feature. Note the library assumes that the sensors are distributed around the home and stream their data to the home server. Since most off-the-shelf sensors have limited filtering capabilities, filtering is best implemented on the home server. When the sensor data arrives at the server, the data are immediately filtered before being stored on the hard drive. The home server then allows only authenticated individuals to configure the filters.

There are a variety of off-the-shelf sensors available for use in the home. These are examples of how the library will provide to the designers mechanisms to filter the data:

- Sample rate: Increase/decrease the rate at which the sensor data is sampled.
- Reduce data precision: Report ranges of sensor data instead of the actual measured value.
- Time ranges: as opposed to timestamps on recorded data, stamp the data with a time range
- Data aggregation: Report aggregate data over time. For example, the number of times a person moved between rooms, instead of a detailed path and timeline of their day.

There are two primary ways a designer will interact with the sensors. The first is to configure the data filters. For example, if a researcher is using a force sensor to determine when an elder moves a pill bottle (and therefore is likely to have taken a pill), reducing the sample rate is not feasible. To increase privacy, some type of data aggregation may be used instead. The second use of the toolkit is to control access the filtered data. The library will provide a set of authentication options and an API to allow only authenticated programs to directly request data from the data store. Thus, if data requirements or analysis change or if an elder recovers from an event or declines, the system need not be entirely redesigned.

The critical element of the framework is that it enhances the elements of each participant. The elder understands her concept of privacy, and the toolkit helps her to articulate this. The designer understands ubicomp, and the toolkit assists him in designing secure and privacy-enhancing systems without requiring expertise in privacy, security and ubicomp. The uniform elements of the library will ideally include some level of interaction design and a split of responsibility between the user (who may be inexperienced with computers) and the designer (who may have no usability expertise).

Acknowledgments

The authors would like to thank Tammy Toscos for editing the final version of this paper and agreeing to present it at the *Nurturing Technologies in the Domestic Environment Workshop*.

Biographical Paragraph

Professor L. Jean Camp's core interest is in the interaction of technical, financial and social trust. It was this interest that led Prof. Camp from graduate electrical engineering research in North Carolina to the Department of Engineering and Public Policy at Carnegie Mellon, and it remained her core interests as a Senior Member of the Technical Staff at Sandia National Laboratories. At Sandia National Laboratories her work focused on computer security. She left Sandia to join the faculty at Harvard's Kennedy School. As an Indiana University Associate Professor in Informatics her research addresses security and privacy as human and technical. She is the author of one book, edited a second, has a third under contract, has more than fifty peer-reviewed publications and more than a hundred written works. Please see <http://www.ljean.com/cv.html> for an up-to-date curriculum vitae.