

Beyond Consent: Implications of UbiComp for Privacy

| | | |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Jean Camp ljean@ljean.com Associate Professor Informatics | Kay Connelly connelly@cs.indiana.edu Assistant Professor Computer Science | Lesa Lorenzen-Huber lehuber@indiana.edu Assistant Professor Health, Physical Education and Recreation |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|

Indiana University
Bloomington, IN

1 Abstract

Ubiquitous computing, or 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.

The ubiComp transformation has the ability to lead us to an Orwellian society where people will no longer be aware when they are interacting with the network and creating data records. The potential negative implications of this are clear, and frightening. However, ubiComp has immense potential to improve lives, including the lives of vulnerable individuals who can leverage the abilities of ubiComp to reach or maintain personal independence and autonomy.

Currently, design for privacy requires a user who understands the social implications of ubiComp technology, demands a design that respects privacy, and articulates specific technical design requirements. Design for privacy also requires a ubiComp designer with mastery of privacy enhancing technologies, security mechanisms, and a profound understanding of privacy. Data protection and fair information practices require a transactional approach to data management, where users make discrete decisions about data flows that are then integration. None of these is an adequate approach to the myriad problems in privacy in ubiComp.

Privacy is a socially constructed value that differs significantly across environments and age cohorts of individuals. The impact of ubicomp on privacy will be the greatest in terms of privacy in home-based health care. Value-sensitive design has the potential to make this transformational change less disruptive in terms of personal autonomy and individual boundaries by integrating privacy into ubicomp home health care. Yet value-sensitive design must be predicated upon a shared concept of the particular value under consideration.

In this paper we provide a high-level overview of the competing concepts of privacy. We critique each of these concepts in terms of its applicability to the specific domain of home-based health care. We also critique privacy as constructed in home-based ubicomp systems, and in ubicomp systems that present themselves as privacy-enhancing. We introduce the strengths and weaknesses of value-sensitive design for the case of ubicomp, particularly in the home. We enumerate the possible interactions between home-based ubicomp, various privacy regimes, and design for values.

We conclude that not only is no single theory of privacy applicable; but also that the knowledge of both the technology and the privacy risks is an unreasonable requirement for ubicomp users and designers. We argue that intimacy of the technology, the continuity of the data flow, and the invisibility of the risk in ubicomp limits the efficacy of data protection and fair information practices. Data protection must be augmented by more subtle mechanisms, and standards of care in privacy design should be developed before the Orwellian default becomes installed base.

2 Introduction

Ubiquitous computing (also called ubicomp) has the potential to serve the needs of the aging population, current trends in ubicomp design have yet to substantively address the inherent privacy challenges. A reason for ignoring the privacy issue to date is that elders lose considerable privacy if they move into a nursing home, but relatively less privacy to ubicomp or other home health care technology [27]. It is likely when threatened with the loss of their independence, most elders will choose the lesser evil: the loss of privacy that comes with monitoring technologies.

Privacy versus ubicomp is a Hobsons choice. The ubicomp projects in this area claim that technology will help family members decide when an elder must be moved to an assisted living facility. So by definition, the technology is being introduced before the elder is faced with the either-or choice presented above. In addition, the technology is presented in its entirety, with potentially privacy-influencing design choices embedded and without the possibility of the participants examination. As such, it is essential that research in this

area address the issues of privacy surrounding sensing and monitoring technologies in the home.

Implementing value-sensitive design requires understanding what a particular value (in this case, privacy) means in the design context [6] [12]. The sheer complexity of understanding a value as amorphous as security, which is itself better specified than privacy, has been a serious difficulty in applying value-sensitive design [15]. In our proposal there is no monolithic perspective on privacy. There are multiple stakeholders in our scenario: the participants and the network of informal caregivers (typically family and friends), each perhaps with distinct and often competing conceptualizations of privacy. In the following sections, we describe the current theories about the nature of privacy, and how these distinct views of privacy alter technical design. We will utilize these theories to construct our initial privacy framework.

3 Data Protection & Fair Information Practices

Data Protection and Fair Information Practices are widely accepted as the mechanisms by which privacy can be protected in practice. A popular evaluation is that when data are protected, privacy takes care of itself. In this section we look at data protection and its interaction with ubicomp.

The earliest instantiation of privacy protection through careful information practices is based in the Code of Fair Information Practice. The Code of Fair Information Practice was offered by the Office of Technology Assessment in 1986 and is a foundation on which subsequent data protection practices have been constructed. The Code (and the related data protection requirements) has as its core transparency, consent, and correction.

In terms of privacy, these are generally seen as a reasonable minimum. However, in the case of designing for home-based medical ubicomp, even the Code, which is far more simple than the European or Canadian data protection regimes, is problematic. Transparency requires that no data compilation be secret. Of course, that is implicit in the installation of a sensor network in ones home.

Consent includes not only the existence of data in sorted form, but also the uses of that data. Consent implies that data can be deleted or corrected when desired by the subject. However, in the case of home-based ubicomp, some combination of caregiver and care recipient action may be necessary. For example, individuals may attempt to hide any increase in impairment by deleting data or increasing filtering to the point where the data are no longer illustrative.

The capacity to alter data, included in the requirement that individuals are allowed to ensure data are correct, obviously has distinct implications when the data are stored lo-

cally and the individual may not perceive correct data as being in his or her own interest. Furthermore, the interpretation and therefore correction of medical data may require personnel about whom there are other privacy concerns. For example, review of one element of data by an insurance entity need not expose all sensor network data to that entity. The need for the privacy toolkit illustrates that the mechanisms used for desktop computers are inadequate to address the subtleties of this agent of change.

4 Alternative Concepts of Privacy

Privacy can be a right to seclusion – “the right to be let alone [31]. Privacy as seclusion is the underlying theory of privacy tort rights. A constant video ubicomp environment would violate the right to seclusion, potentially even when the system allows for the preservation of anonymity. Consider, for example, ubicomp in a bathroom. Accurate depictions would violate privacy in the sense of seclusion even without the association of a unique name to any user. Yet ubicomp in such a location may be necessary in a home health care system; for example, the bathroom is a common location for falls. Some activities that need monitoring are necessarily (e.g., hygiene) or commonly (e.g., taking medication) localized to the bathroom.

Privacy is a form of autonomy because a person under surveillance is not free. In the United States, Constitutional definitions of privacy are based on autonomy, not seclusion. These decisions have provided both sexual autonomy and, in the case of postal mail and library records, a tradition of information autonomy (This concept of information autonomy was altered under the USA PATRIOT Act.). In technical systems, privacy as autonomy is usually implemented as strong anonymity. iPrivacy offered to hold all consumer information and thus be left alone. To the extent that the ubicomp addressed shared social as well as private family spaces, we will also be informed by theories of social privacy. Privacy can also be considered a property right, and as such, control over privacy can yield economic advantage to select stakeholders [3] [22]. For example, ubicomp that provides demographic information and thus enables price discrimination can violate this dimension of privacy. In this case, the data are economically valuable and thus centralized authorities will have economic incentives to share those data [24]. Recognizing that these models of privacy exist is not to dictate design specifics. Autonomy is too subtle to be addressed via a single computational mechanism. Privacy as the right to seclusion fits under the boundaries model. Privacy as property in ubicomp would require either too much contractual overhead or a ubiquitous digital currency with very low computation requirements. Yet each of these perspectives can assist in informing designers about privacy implications and help participants articulate privacy concerns.

Most often, privacy in ubiquitous computing is spatial, conceived of as an issue of bound-

aries [17] [19] [4] [14]. Many ubicomp designers have adopted a concept of contested social spaces as articulated in the concept of privacy as process [2]. The idea of contested space is particularly useful in public spaces, where there is an issue of privacy in public, often examined under the rubric of social privacy. As our area of focus is home-based ubicomp social privacy plays a correspondingly smaller role, with the primary issue of social privacy being on data compiled on guests in the social area of a home.

The boundary concept strongly parallels the early work on regulation of speech on the Internet, in which legal and policy scholars disputed the nature of cyberspaces, e.g. [23] [30]. This debate was settled when Internet Service Providers obtained a Safe Harbor provision in the Digital Millennium Copyright Act that delineated appropriate ISP behavior with regards to copyright (a most troublesome modern speech/property conflict) and expression. In both cases, spatial metaphors were adopted because of the potential power of the heuristic. Spatial metaphors offer great subtlety. Like the speech debate, the spatial ubicomp privacy discourse has integrated issues of social, natural and temporal spaces [19]. Again mirroring the speech debate, ubicomp researchers are finding that while spatial metaphors offer insight, they offer little practical design guidance.

The distinction between virtual and physical spaces is essentially the nature of the boundaries that divide them. Virtual boundaries are distinct in three dimensions: simultaneity, permeability and exclusivity [8]. Simultaneity refers to the ability of a person to be two places at once: at work and at a train ticket booth. Permeability is the capacity of information and communications technologies (ICTs) to make spatial, organizational or functional barriers less powerful or even invisible. The permeability of the work/home barrier is most clearly illustrated with telecommuting. Exclusivity, in contrast, is the ability of ICTs to create spaces that are impermeable, or even imperceptible, to others. Intranets may offer exclusive access through a variety of access control mechanisms, and the creation of databases that are invisible to the subjects clearly illustrates the capacity for exclusivity. In the physical sphere, the walled private developments offer an excellent example of exclusivity, yet it is not possible to make physical spaces so exclusive as to be invisible. Technologies redefine the nature of space, and digital networked technologies alter the nature of boundaries. [28]

The technologies developed in this project will be researched with an understanding of the data protection and boundary concepts of privacy but grounded in concepts of autonomy, seclusion and property. This research is focused on design for values rather than post-hoc evaluation of design (although evaluation of the prototypes is a critical part of the evaluation process). Different technologies implement different concepts of privacy. For example, the Zero Knowledge System, (ZKS) a privacy services company which offered complete data privacy even from the servers at the company itself. ZKS offered autonomy through anonymity. In contrast, the competing consumer system, iPrivacy, offered escrowed data, which is a seclusion privacy solution, to prevent later spamming of the customer. ZKS

required trust only in the underlying technology, while iPrivacy concentrated trust in its corporate parent [9]. ZKS allowed people to participate with cryptographically secure pseudonyms. In contrast, the framework is expected to illustrate how a particular sensor might function in any environment, with the designer and the subjects bringing the subtleties of the spatial considerations to the framework.

5 Privacy in UbiComp Design

Value-sensitive design is a design method whereby the initial design is accompanied by a values statement. The values statement is explicitly not a Software Development Impact Statement because, while values choices can be made in design, value choices can also emerge during use. Design for values as a method embeds explicit values choices, documents those choices, and thus enables adoption and alteration of technologies to be explicit choices made in a larger social context. Design for values is not exclusively technologically deterministic. The technologically deterministic [10] [21], socially constructed [11] and dynamic iterative [18] models of technological development have clear parallels in, respectively, the technical, preexisting, and emergent models proposed for computing systems in design for values [13].

Technical bias is that which is inherent in or determined by the technology. Preexisting bias is that bias which had been previously socially constructed and is integrated into the technology. Emergent bias develops as a system is used and develops in a specific social context. The goal in value-sensitive design is not to create omniscient designers, but rather ethical design (within the designers informational space) that enhances social discourse about any specific technological artifact.

Clarification of values is particularly important in discussing security and privacy, as these are so often confused in technical design [1]. While computer security and privacy are, in most cases, well aligned, they are not equivalent. Security is the control of information. Privacy is the control of information by the subject of the information. Security can provide tools for anonymizing data, so that privacy is not a concern. However, authentication is also a pillar for security. Authentication can diminish or eliminate anonymity (Note that there are anonymous identity token, e.g., digital cash, that provides authentication of an attribute but not authentication of identity.). Security technologies enable authorization, identification and verification of identity. With personally identifiable information, the inability of the subject to control information linked with his/her identities is a threat to privacy. Authentication systems have been shown to decrease security and threaten privacy by implementing too broad a concept of identification in their design [7]. This is most clearly illustrated in the widespread use of social security numbers as a mechanism for authentication, and the resultant identity theft.

In fact, some work on security in ubicomp has been in direct opposition to privacy. For example, in one design, the addition of access control to location systems concentrated data rights by creating a centralized authority. This removed the right of the individual to control his or her own information by having institutional policies apply to individuals, and having spatial policies that override personal policies. Indeed, the potential privacy and personal security threats are exacerbated in this system because the individual requesting data is anonymous while the person whose location information is provided is both identified and incapable of knowing when he or she is identified [16]. By implementing a narrow concept of centralized access control as security, this system has increased exposure of personally identifiable information, prohibited opt-out, and decreased individual autonomy. The stated goal of these designers was to add security, so that control could be increased. Yet ignoring privacy resulted in a mutual-surveillance panopticon.

In other cases, innovative security work expands the options in ubicomp, but in doing so creates a new set of risks. For example, one design for security in ubicomp is the mother duckling model [?]. In this model, a device is imprinted by a central device upon initiation (waking) and responds only to that device, as a duckling is imprinted by its mother. The ability to re-initialize a device (e.g., resurrect a duckling) creates some security risks through denial of service via resource exhaustion. Such a denial of service attack may be particularly problematic in a medical monitoring system where reliability concerns may trump security concerns. In one situation, it may be better for a device to fail and the failure brought to the attention of a responsible party than to risk device hi-jacking by re-initialization. In another situation, it may be better for there to be a loss of privacy than a loss of functionality, so security risks are rejected over resource loss.

Privacy by design, as in the Cricket system, enables both location services and individual privacy. In this case, the location offers relevant information that can be requested by users. The only authorization required is physical location. Therefore, by using verifiable assertion of location, the location service can determine the authorization required for data access, and the default is anonymity of the requestor. In this case the data are public (e.g., relative location, available nearby services such as food). The individual is able to access information based on the relevant information (i.e., location) without losing privacy. The Cricket system implemented an autonomy model of user interaction where users could be anonymous and still access data. The Cricket designers did not use an explicit value-sensitive design approach, but did effectively and explicitly design to value privacy.

While there is no known predictable method for making an absolute assertion about the privacy implications of a given default in a particular feature for a generic system, clearly predictions can be made about the potential for privacy violations created in a particular technology [5] [20]. Although much research on privacy is applicable to ubiquitous computing and there are nearly 150 privacy enhancing technologies on the market, as well as many tens of innovations submitted every year to the Privacy Enhancing Technologies

Workshop, there has been almost no work on examining these issues in the context of home-based ubicomp for care-giving, potentially one of the most extreme cases in terms of privacy. An exception is Intel's CareNet project, which performed extensive user studies which included examining the issues surrounding privacy with home-based ubicomp. Unfortunately, they simulated the sensor network and thus privacy issues that may have emerged during deployment could not be considered.

6 The Perfect Privacy Storm

The implications of ubicomp in terms of privacy will be of particular importance in another area of transformational change: the rapidly aging population. As the numbers of elders increases, 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. 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 [25]. 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 [26].

The combination of a vulnerable population, embedded computing, and inadequate privacy regimes may lead to a digital perfect storm. An obvious threat is financial fraud enabled by the combination of cross-border data flows (legal or otherwise) and international financial opportunities.

Loss of privacy and detailed data surveillance is not a requirement for ubicomp, if the designers are aware of the reason for the technology and design accordingly. 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 lay user to analyze the pressure sensor, filters and possible application, in terms of their own homes and lives?

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. Our hypothesis is that autonomy implicitly requires filtering. 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. Autonomy is a unique challenge,

as to ask, What exactly is it you do not want us to learn? is in inane any case, but in privacy research such a question is a particular oxymoron.

From the paradigm of privacy as seclusion comes the right to be let 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 a higher level of checking? For example, gait identification in the home may be something that comforts the elder in the evening by identifying thumps in the night as the caregiver or the cat, but not an element which is desirable during more social daylight hours. However, the evening higher level of data might not be shared or the daytime level of data depending upon the individuals elders sense of being left alone or subject to surveillance by the ubicomp. The privacy as property paradigm brings forward not only the alienable nature of data but the idea of the right to exclude.

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 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; better or worse balance in a given time period. Spatial questions can also assist in defining data boundaries. 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? And if so, to whom, bringing back the details of property-like exclusion.

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? The data protection emphasis on visibility may not be appropriate for livable home-based ubicomp, as people may become tired of consciously interacting with the technology on a day-to-day basis. Other questions from data protection demand the reasons for data compilation and a firm deletion date.

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 for elders and their caregivers. In an invisible design, sensors placed where medicine is kept and taken can detect if a person did not follow all the instructions, take the incorrect dosage, take doses at the wrong time or in the wrong combination. In a visible design, users can indicate how and when they have taken medication by pressing buttons on a personal hand-held device. [29]

Ubicomp can be used to monitor symptoms of actions as opposed to actions. For example,

a changed heart rate can be associated with dehydration, infection, wrong medication, overdose of medication, or some form of stress. A heart rate monitor can be used to measure this aspect of physical well being. One design might place the heart rate monitor in a T.V. remote, thereby measuring an elders heart rate invisibly whenever they use the remote. Another design may place a heart rate monitor in a button that the elder is reminded to push every morning when they are fixing their breakfast. The second design is visible, the first is integrated.

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?

7 Closing

UbiComp is an agent of change. The impact of ubiComp as a large-scale transformational change will be the greatest in terms of privacy in home-based health care. Value-sensitive design has the potential to make this transformational change less disruptive in terms of personal autonomy and individual boundaries by integrating privacy into ubiComp home health care. Yet value-sensitive design must be predicated upon a shared concept of the particular value under consideration. We posit that a single framework built on the technology and the various concepts of privacy inform both designers, for value-sensitive design, and participants, for their own autonomy.

There are numerous pressure sensors and as many combinations of risks and applications as there are elders. It will require more than the law or technologists alone to develop a meaningful framework that provides a cooperative, elder-informed, iterative understanding of the concerns of caregivers and participants for sensors in each space, for each risk set, and for each application. Technologists and lawyers can begin now to examine ubiComp as it is being developed and designed.

Demographic changes, longer life-spans, 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. Simultaneously other demographic changes (e.g.,

families living further away from each other, increased necessary participation of women in the paid work force) have complicated informal care giving.

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. Studies such as ours will contribute to the development of privacy-sensitive ubiComp design, and that, more importantly, can enable independent living for the elderly and disabled.

References

- [1] P. E. Agre and M. Rotenberg. *Technology and Privacy: The New Landscape*. The MIT Press, 1997.
- [2] I. Altman. *The environment and social behavior*. 1975.
- [3] E. Bloustein. Privacy as an aspect of human dignity: an answer to dean prosser. *New York University Law Review*, pages 962–970, 1968.
- [4] M. Boyle. A shared vocabulary for privacy. In *Privacy in UbiComp*, 2003.
- [5] L. J. Camp. *Trust and Risk in Electronic Commerce*. The MIT Press, 2001.
- [6] L. J. Camp. Design for trust. In R. Falcone, editor, *Trust, Reputation, and Security: Theories and Practice*. Springer-Verlag, 2003.
- [7] L. Jean Camp. Digital identity. *IEEE Technology and Society*, pages 34–41, 2004.
- [8] L. Jean Camp and Y.T. Chien. the internet as public space: Concepts, issues and implications in public policy. In R. Spinello and H. Tavani, editors, *Readings in Cyberethics*,. Jones and Bartlett Publishers, Sudbury, MA, 2001.
- [9] L. Jean Camp and Carlos Osorio. Privacy enhancing technologies for internet commerce. In Rino Falcone, editor, *Trust in the Network Economy*. Springer-Verlag, 2003.
- [10] E. Eisenstein. *The printing press as an agent of change*. 1979.
- [11] C. S. Fischer. *America calling: A social history of the telephone to 1940*. 1994.
- [12] Batya Friedman. *Human Values and the Design of Computer Technology*. University of Chicago Press, 2001.
- [13] Batya Friedman and Helen Nissenbaum. Bias in computer systems. *ACM Transactions on Information Systems (TOIS)*, pages 330–347, 1996.

- [14] J. Geraci. Community and boundary in the age of mobile computing: UbiComp in the urban frontier. In *Privacy in UbiComp*, 2004.
- [15] E. Felton H. Nissenbaum and Friedman. Computer security: Competing concepts. In *The 30th Research Conference on Communication, Information and Internet Policy*, September 2002.
- [16] U. Hengartner and P. Steenkiste. Implementing access control to people location information. In *9th Symposium on Access Control Models and Technologies*. 2004.
- [17] X. Jiang. Safeguard privacy in ubiquitous computing with decentralized information spaces. 2002.
- [18] Jay Kesan and Rajiv Shah. Establishing software defaults: Perspectives from law, cs, and behavioral economics. *Illinois Law and Economics Working Papers Series*, 2006.
- [19] M. Langheinrich. Privacy invasions in ubiquitous computing. 2002.
- [20] L. Lessig. Code and other basic laws of cyberspace. 1999.
- [21] M. McLuhan. The gutenbergs galaxy. 1977.
- [22] P. Mell. Seeking shade in a land of perpetual sunlight: privacy as property in the electronic wilderness. *Berkeley Technology Law Journal*, pages 11–92, 1996.
- [23] E. J. Naughton. Is cyberspace a public forum? computer bulletin boards, free speech and state action. *Georgetown Law Journal*, pages 409–441, 1992.
- [24] Andrew Odlyzko. Privacy, economics and price discrimination on the internet. In L Jean Camp and Stephen Lewis, editors, *Economics of Information Security*, volume 12 of *Advances in Information Security*, pages 187–212, New York, NY, 2004. Springer.
- [25] US Government Accountability Office. Long-term care: Diverse, growing population includes americans of all ages. Technical report, Washington, DC, 1998.
- [26] US Agency on Aging. Profile of older americans. 1998.
- [27] P. E. Ross. Managing care through the air. *IEEE Spectrum*, pages 26–31, 2004.
- [28] S. Shapiro. Places and space: The historical interaction of technology, home, and privacy. *The Information Society*, pages 275–284, 1998.
- [29] Frank Stajano. The resurrecting duckling. pages 204–214, 2000.
- [30] A. Sterns. Curriculum design and program to train older adults to use personal digital assistants. *The Gerontologist*, pages 828–834, 2005.

- [31] Cass Sunstein. The first amendment in cyberspace. *Yale Law Journal*, pages 1757–1804.
- [32] S. Warren and L. Brandeis. The right to privacy. *Harvard Law Review*, pages 193–220, 1890.