Reflecting on the Invisible: Understanding End-User Perceptions of Ubiquitous Computing

Erika Shehan Poole, Christopher A. Le Dantec, James R. Eagan, and W. Keith Edwards

GVU Center and School of Interactive Computing
Georgia Institute of Technology
85 Fifth Street NW
Atlanta, GA 30308 USA
{erika, ledantec, eaganj, keith}@cc.gatech.edu

ABSTRACT

How can designers of ubiquitous computing technologies ensure that they understand the non-functional needs, values, and expectations of end-users? In this paper, we use a qualitative method from public policy to elicit reflective feedback from end-users about technologies that they may not yet have used nor fully comprehend. Our study uncovers information about end-user perceptions of RFID, including a range of "folk theories" held by the public about this technology, and their associations of it with certain social groups and values. We argue that these perceptions can limit technological adoption, and conclude with a discussion of challenges for the design and deployment of ubiquitous computing systems.

Keywords

evaluation techniques, folk theories, qualitative methods, social implications, technology adoption

ACM Classification Keywords

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

INTRODUCTION

Evaluations of ubiquitous computing systems have typically examined the *functional* aspects of these technologies. A system's success has historically been judged based on factors such as performance, utility, or usability. All of these aspects of a technology are essential components to its ultimate success or failure; a technology that neglects performance, utility, and usability is unlikely to be adopted.

Yet *non-functional* criteria also influence, and even determine, the ultimate success or failure of a technology. Non-functional criteria include such factors as the association of a technology with certain ethical or value judgments in the minds of its users, affiliation of a technology with particular social groups or subcultures, perceptions of the social appropriateness of a technology in various contexts, and understandings (or lack thereof) of the internal workings of a technology. Yet how can designers uncover these non-functional beliefs and associations? Answering this question is especially problematic with emerging ubiquitous computing technologies, as people may not have used the technology in question nor fully understand it. Are there methods we can use to allow these potential users to provide reflective feedback on their perceptions of a novel, unfamiliar technology?

In this paper, we investigate how designers can better understand the non-functional aspects of end-users' engagement with emerging ubiquitous computing technologies. Using a qualitative technique originating in the public policy research community [25], we show how to elicit deep reflection from end-users around their perceptions of ubiquitous computing, and explore how these perceptions can affect adoption and use. The technique we use provides a way to explore a richer range of users' associations with a given technology without leading biases and without constraining the language that participants use when discussing the technology.

We ground our discussion by presenting the results of a qualitative study investigating public perceptions of Radio Frequency Identification (RFID) technology. This technology has been used as a building block for a number of ubiquitous computing research applications as well as in commercial deployments. Despite its widespread use, however, RFID remains invisible—both physically and in interaction—to end-users. It has also been the source of negative attention by popular media and some civil liberties organizations. Hence, we find it to be an ideal point for opening a discussion about understanding end-user perceptions of ubiquitous computing technologies. In particular, we examine folk theories commonly held by the public about the capabilities, applications, and appropriateness of RFID. We also examine public perceptions of how RFID may support or detract from personal and shared societal values.

UbiComp'08, September 21-24, 2008, Seoul, Korea.

In the next section, we present a concise overview of related work on understanding non-functional aspects of technology adoption and use, and provide a brief primer on RFID technology. We then discuss a method for engaging the public in discussions about their perceptions of ubicomp technologies. Next, we explain how we used this method to study preconceptions, value associations, and social affiliations perceived to be present in RFID. We conclude with implications for the design and deployment of ubiquitous computing systems using RFID and similar technologies.

RELATED WORK

In this section, we discuss related work focused on non-functional concerns in technology adoption, social implications of ubiquitous computing, and folk theories of science and technology.

Non-Functional Concerns in Technology Adoption

Prior research in Human-Computer Interaction (HCI) demonstrates that factors *external* to a given technology may influence a technology's adoption, use, and eventual success or failure. For instance, Voida et al.'s study of iTunes showed how non-functional factors such as identity management (the work of controlling or shaping others' perceptions of ourselves, in this case through editing of shared playlists to convey "coolness") influence how users interacted with the software [13,34]. In another example, Gaw et al. examined how non-functional factors affected the adoption and use of email encryption [12]. While poor usability of email encryption is a well-understood barrier to adoption [37], Gaw et al.'s study of a political activist organization showed that users' associations of encryption with certain values, social groups, and traits also influence adoption and usage patterns. Participants saw everyday use of encryption as "abnormal" or "paranoid," further deterring usage. Likewise, encrypting a message also served as a signifier of its importance, a fact that meant users were unwilling to encrypt "unimportant" messages for fear of risking the ire of their colleagues. In these cases, the non-functional aspects of the technology proved to be a better predictor of adoption than usability or technical capabilities. Similar findings have been demonstrated in studies of organizational uptake of collaboration technologies (cf. Orlikowski and Gash's study of Lotus Notes adoption [28]).

Outside of HCI, a number of researchers have examined how factors beyond functionality, performance, or usability shape technology adoption and acceptance. Notably, work in the area of science and technology studies emphasizes the role that users' (and non-users') perceptions have in technology adoption, and how these flexible and varied interpretations impact use (cf. Bijker's account of the development of the modern bicycle [2]). Likewise, the field of cultural studies has explored how culture impacts technology use, including portrayals of technology in the media (such as marketing, news reports, and movies), how technologies come to be identified with particular subcultures, and how values become associated with certain technologies (cf. [7,16]).

This prior research highlights the role that non-functional aspects have in determining the adoption, use, and eventual success or failure of a technology. In many cases, such non-functional aspects overshadow issues such as technological features, performance, or usability. Prior research also points to the difficulty of understanding these non-functional aspects in a way that is actionable for design. In the case of the examples cited from the HCI community, the technologies under study were both well-understood and in common use; in contrast, it is unclear how we might understand perceptions around *emerging or unfamiliar* technologies, especially ones for which users may have difficulty articulating their beliefs. Likewise, in the work from historical and cultural studies, insights about user perceptions are often derived retrospectively, though analysis of documentary evidence after the fact. These bodies of work provide little insight into how we might use an understanding of these perceptions to *inform future design work*.

Social Implications of Ubicomp: Engaging the Public

A number of researchers have discussed larger social implications of RFID-tagged ubiquitous computing environments. These researchers have focused particularly on issues related to information security, privacy, and technology paternalism [1,15,19,22,23,30,31]. In contrast, our study aimed to understand end-user perceptions of RFID beyond these issues, and to explore a method useful for understanding public perceptions of technologies besides RFID.

More generally, research focused on understanding the relationship between human values and computing systems is ongoing in HCI and ubiquitous computing. In particular, Value Sensitive Design (VSD) defines a framework to investigate and expose the human values embodied in technical systems [11]. While VSD provides a lens for examining values in system design, the exact empirical tools a researcher or designer might use to gain a better understanding of human values is left open-ended. This open-endedness encourages adopting techniques from other domains, such as sociology and public policy, to explore how human values affect the domain in question. Our work can be used within the VSD framework, but it would also be appropriate for other design frameworks that engage the public and system designers in discussions about the larger social implications of future technologies.

In a complementary approach to our work, Nathan et al. argue for more public input and engagement in the design and deployment of ubiquitous systems [27]. In particular, they argue that designers need to be aware not only of end user values, but of the long-term, systemic effects of ubiquitous computing technologies. They suggest using scenarios describing future uses of technologies (that show unintended consequences of the technology) to guide designers in discussions about societal implications of

technology. However, unlike in Nathan et al.'s work, we use photos of objects, people, environments, and situations that are common today.

Folk Theories of Science and Technology

In our study, we examine folk theories that the public holds about RFID technology. Folk theories, as first described in Kempton's study of household thermostats [20], are ways of understanding the world that are shared by a social group, and are based on one's personal experiences or social interactions. While they are not completely accurate accounts, these theories can provide people with explanatory power, can guide behavior surrounding use of the technology, and can allow people to make predictions about how a technology will function under certain conditions.

Lay understandings of complex phenomenon have been studied in other fields, particularly in physics [17], geography [8], and earth science [35]. In education, knowledge of these lay understandings can lead to more appropriate teaching methods [35]. In public health, understanding folk theories of natural and technological risks can help with the creation of informational materials that are useful, believable, and understandable to the public [25].

Recently, a number of researchers have examined folk understandings of computing, particularly in the areas of networking and security. Friedman et al. studied how people understand web security [10]. Poole et al. studied how people perceive of home computer network structure [29]. Yan et al. studied how children conceive of the Internet's structure [38]. Hendry studied lay understandings of search engines [18]. While these studies focused on lay understandings of computing, our work differs in that it explicitly examines how these lay understandings may impact attitudes toward or willingness to adopt of the technologies in question.

Radio Frequency Identification (RFID): A Quick Primer

In this section, we discuss RFID in terms of its functional aspects and applications, and describe how our work differs from existing studies of usability and acceptability of RFID.

Functional Aspects of RFID

RFID is a family of technologies that allows data to be stored on a small device and communicated to another device using radio waves. RFID systems have two main components: a *tag* and a *reader* [3]. The exact capabilities of a tag can vary; at the minimum, a tag contains an antenna and a semiconductor chip encased in forms that can be smaller than 1cm in size. Tags can be either *active* or *passive*. Active tags require a power source. Passive tags do not have their own power source, but are powered by electromagnetic waves emitted from readers. The range at which a tag can be read depends on the design of the particular RFID system, but is generally limited to a few meters [36].

RFID does not require line of sight to operate, hence tags can be physically built into objects, making them "invisible" to an end user. This quality offers potential functional benefits—along with radically different affordances—over barcodes, data glyphs, or other visually-based data encoding technologies. Some tags can only have data written to them at the time of manufacture, but others can be rewritten. In addition to storing data, some tags have limited data processing capabilities to facilitate security measures such as encryption or sensors that measure environmental conditions. Depending on the RFID application, readers may possibly forward received data over a network to outside applications or databases in order to access additional information. For example, tags often contain data that is treated as an index into a database to retrieve data records too large to store on a tag.

RFID Applications

Perhaps the primary driver for RFID deployment lies in its benefits for commercial and government applications, most notably in the context of supply chain management [36]. RFID tags can be incorporated into building access cards, credit cards, and in automatic highway toll collection systems [36]. Australia, the United States, and the European Union all have adopted RFID as a means of electronically encoding identifying information into identity documents such as passports [32]. In such applications, the information stored on tags may represent account numbers, identity numbers, and other information that directly corresponds to their human owners. RFID is also used in living organisms. For example, pets or livestock may have subdermal RFID tags inserted for identification purposes [36]. The use of RFID in humans, although still rare, is becoming more common [33]; these tags have been used in applications ranging from storing medical information about individuals to allowing VIP access to nightclubs [26].

RFID User Studies

A number of researchers have examined user orientations toward RFID-based technologies. Günther and Spiekermann [15] and Rothensee and Spiekermann [30] have examined how German consumers orient toward RFID and privacy concerns in retail environments. Their studies, however, focus primarily on reactions to RFID when used in retail environments rather than broader applications or perceptions of the technology. In contrast, our study focuses on user perceptions of RFID in a wide range of environments. Mäkelä et al. [24] studied the usability of RFID technologies through an experiment in which Finnish consumers interacted with RFID-tagged posters. Their study focused specifically on usability issues, and revealed that users have difficulty understanding how RFID functions. However, their study was limited to one particular application of RFID and did not examine non-functional aspects of the technology such as attitudes or values.

A number of studies have focused on privacy aspects of ubicomp and RFID technologies, with many proposing technical approaches to increasing privacy protections (see, for example, [9,19,21,23]). Privacy can certainly be an important factor in determining the public's acceptance of a given emerging technology; however, *perceptions* of privacy (or lack thereof) afforded by a given technology are also important. Further, our work shows that privacy is only one of many concerns the public may have about RFID.

METHODS

To study public perceptions of RFID technology, we adapted a technique used primarily in public policy research. This technique uses a combination of semi-structured interviews and photo elicitation exercises to study perceptions of complex concepts that are often difficult for study participants to verbalize (for instance, the risks of living near power stations or having radon in one's home) [25]. By using this technique, which we describe in-depth below, we were able to engage participants in a discussion about the social implications of ubiquitous computing and uncover commonly held folk theories about RFID.

During the study, participants completed a semi-structured interview as well as a photo elicitation exercise in which they discussed a series of photos representing a broad spectrum of objects, places, and situations they might encounter in their daily lives. The interviewer informed participants that some photos may be associated with RFID and some may not. For each photo, the interviewer asked them to say whether they thought that object, place, or situation was associated with RFID and why. We found the photo elicitation component essential; especially for people who claimed they had never heard of RFID, having pictures as a reference jogged their memories and provided a comfortable grounding upon which they could discuss their opinions about RFID (and technology in general) in concrete terms rather than as an abstract concept. In fact, although many of our study participants initially claimed to know nothing about the technology and have no opinion of it, during the photo elicitation exercise these same users began to reveal a range of opinions and perceptions about the technology. Interviews without the photo elicitation exercise would have been unlikely to yield such rich results.

Additionally, through this combination of having an artifact upon which to ground the discussion as well as encouraging the participants to discuss whatever came to their minds for each picture—even if it seemed silly, outlandish, irrelevant, or incorrect—we created an opportunity for participants to reflect and talk at length about RFID.

From a methodological perspective, this photo elicitation technique yields particular advantages over research instruments such as questionnaires. While questionnaires are often used to gain insight into beliefs, and can be quick to administer to a large number of subjects, they have significant limitations, especially in the context of ubiquitous computing. Specifically, questionnaires may only focus on a narrow set of beliefs and misunderstandings that people have, and do not allow for exploration of issues of which the researcher designing the study is unaware. Additionally, questionnaires and highly structured interviews may use unfamiliar terminology, preventing the respondent from fully reflecting on the technology in question. Moreover, structured testing and questionnaires can unintentionally "taint" study subjects by communicating knowledge about the technology at hand by providing numerous cues and hints [25]. In comparison with techniques such as scenarios, interviews driven by photo elicitation can yield open-ended data beyond the particular case considered by the researcher when creating the scenarios. Additionally, in cases where scenarios have high production values, such as the video scenarios used by Rothensee and Spiekermann [30] and Günther and Spiekermann [15], this technique may also be less expensive and time-consuming. Finally, in comparison to using wizard of oz studies or design probes for design concepts, this technique can be used earlier to gather formative data on users' orientation towards a technology without requiring the time and cost associated with the creation of design prototypes.

Data Collection and Analysis

Twenty-five people in the United States and ten people in the United Kingdom participated in our study. We recruited using word of mouth referrals in the US and UK and by recruiting people attending a festival in a major US metropolitan area. The recruiters informed participants that the study involved completing an interview focused on their opinions about technology. Interviews ranged in length from 30-90 minutes. We transcribed the interviews and coded them for information about how study participants thought RFID functioned, any applications they believed used RFID, perceptions of how data is stored or communicated on RFID tags, who they thought could obtain access to data from RFID tags, comparisons made to other technologies, and any other concerns voiced about RFID including those related to health, environment, privacy, and civil liberties.

Directly prior to the interview, participants filled out a questionnaire that asked them about demographic data, technology experience, attitudes toward privacy, and whether they had ever knowingly used RFID-based technology. The interview began by first asking participants if they had ever heard the term RFID, and if so, what they had heard about it. The interviewers probed for additional information until interview subjects told all they could tell. The interviewers were neutral and non-judgmental, and did not place any constraints upon participant responses, nor did they attempt to steer the conversation in any particular direction. Rather, the interviewers encouraged the participants to discuss whatever came to their minds regarding RFID.

Additionally, this portion of the interview served as a calibration exercise. It helped the interviewers understand terminology that participants used to discuss RFID. The interviewers could then adapt any responses so that they mirrored the participant's language. For instance, if the participant talked about "chips" the interviewer would refer to RFID as a "chip" during the interview. Participants then completed a photo elicitation exercise in which they were asked to sort through a photo set and explain whether (and why) they thought the object, place, or situation was related to RFID or not. The sets each contained 72 photos and used locally relevant images (e.g., photos of retail stores such as Wal-Mart in the US and ASDA in the UK). The photos included:

- Adults and children engaged in everyday activities such as waiting for a train, eating, attending sporting events, watching television, playing cards, or placing items in trash cans
- Currency and credit cards
- Passports and other identity documents/cards
- Buildings such as retail stores, well-known government landmarks, offices, schools, warehouses, and factories
- Weather and nature scenes
- Various high- and low-cost consumer products, including foods, food packaging, and electronic items such as microwaves, televisions, cellular phones, hands-free phone sets, and mp3 players
- Medical supplies and scenes of people receiving emergency medical treatment
- Pets and livestock
- Various modes of transportation including bicycles, cars, buses, trains, airplanes, and spacecraft

After completing the photo elicitation exercise, we asked the participants a set of questions about RFID's role in society (e.g., is it something that society should be concerned about or something that is not really important?) We also asked participants to provide explanations of whether (and why) they thought using RFID was more or less risky than other technologies and artifacts that may store or transmit personal information, such as credit cards, supermarket discount cards, global positioning systems (GPS), and mobile phones. Finally, the interviewers optionally debriefed participants on RFID.

RESULTS

In this section we discuss the findings from our study. We discuss the folk theories or internal accounts our participants held about RFID, how they learned about RFID, their beliefs about the social appropriateness of various applications of RFID, and their perceptions of trust, accuracy, and access to data shared via RFID.

Our 35 participants ranged in age from 18 to 71, and consisted of 14 males and 21 females. Participant occupations included student, salesperson, supermarket clerk, biologist, stay-at-home mother, travel agent, attorney, public health analyst, administrative assistant, marketer, and IT professional. Only 20% were able to identify that they had personally encountered RFID prior to the interview, though over two-thirds had unknowingly encountered the technology in their daily lives.

Folk Theories of RFID Technology

Users' perceptions about what a technology does and how it works shape their orientation towards it. Overall, participants showed significant confusion about what RFID is and how it functions, despite many having either first-hand experience with the technology or exposure through media reports describing it. Even participants who described themselves as technically inclined or had degrees in engineering or technology were not immune to this uncertainty. Confusion ranged from basic misunderstandings about the communications structure of the technology itself (Do the tags broadcast information or receive information?) to uncertainties about capabilities (Do tags have to be touched in order for communication to occur?) to basic lack of familiarity with other details of the technology (How long do tags last? How much do they cost to put into products? How big or small are tags?).

Despite the confusion that participants had about the capabilities of RFID, many could describe the technology by analogy. These analogies formed "folk theories" for the participants, guiding their orientation and understanding of the technical capabilities of RFID.

RFID as Long-Distance Tracking and Communication

Many people believed that RFID can be used to remotely track the location of tagged objects, people, or animals. Conflating RFID with global positioning system (GPS) technology was frequent. Particularly, many participants believed that satellites could be used to track RFID tags in arbitrary locations.

> P15: I'm thinking that maybe you can put this in your dog? A little chip? Though if you were to lose your dog you can track it through satellite or something like that.

In addition to location tracking, many participants assumed that data stored on RFID tags could be remotely read or written to at a large distance.

> P6: Well, whoever the powerhouse is running this device, can, you know, if they can access it or update information on it, I'm assuming they have control to turn it on or off, through some sort of remote technology, like a computer or a satellite.

Participants were mixed as to whether RFID was a technology that continuously broadcasts information, or whether it was a technology that only provided information upon request. Many were also uncertain as to whether RFID tags could be deactivated.

RFID as a Binary On/Off Switch

Some participants likened RFID to anti-theft systems used in retail settings. In this view of RFID, it is a technology that has two states: on or off. Using this folk theory, RFID tags do not contain any unique information or identifiers.

RFID as a Serial Number

On the other hand, a few participants thought RFID was a serial number. As one participant stated:

> P10: I just feel like money might be [RFID] because it's got the codes on it. Anything with a code I feel like fits. And it's got like coding on it. And if you steal money from the bank it all has like codes and numbers and they can like track those numbers.

RFID as Data Storage

Perhaps most commonly, however, a number of participants described RFID as being a device that can hold a small amount of variable information that may or may not be unique, highlighting that—for at least some users—the folk theories they subscribe to about RFID are at least partially correct. People holding this view of RFID often compared RFID to magnetic strips used on credit cards or barcode labels on retail products, although some users holding this view were confused about how RFID differed from these technologies.

Sources of Information about RFID

Perceptions about RFID were, for many of our participants, shaped by the technology's depictions in popular culture, particularly mass-market entertainment. For example, several study participants not only developed their perceptions of RFID from watching science fiction movies, but also used movies as a grounding point for discussing RFID. For example:

> P14: As long as they're not putting it into people like that Will Smith movie where they knew where everything was.

Participants also reported learning about RFID from family, friends, or news media reports of current or potential RFID deployments in retail settings, public transportation systems, or government-issued identity documents. Their knowledge about such deployments was vague, however, and did not seem to translate into well-formed models of how the technology worked or what its capabilities were.

> P12: Well, um, slightly I've heard of it [RFID] Most people that I hear talking about it, like I've said, have a problem with it…It sounds somewhat close to invasion of what I would probably consider private. Privacy...that's pretty much all I've heard of it so far.

Some had learned about RFID applications in the context of their jobs. In particular, a participant who worked in marketing (P4) was aware of RFID use by retailer Wal-Mart, and a participant who worked for a vehicle manufacturer (P3) was aware of applications for monitoring vehicle tire pressure. Although they were vaguely familiar with these applications, neither could explain how these technologies operated in a systematic way.

Over two-thirds of our participants had direct, personal experience with RFID, most frequently by either using an RFID-tagged public transportation fare card or owning a pet with an RFID microchip. Yet even these participants exhibited significant confusion about capabilities of RFID; for example, a number of dog owners believed that their animals' microchips allowed for tracking of lost pets via satellite systems.

Social Appropriateness

Study participants were familiar with a number of RFID applications. They commonly discussed pet microchips, electronic toll payment systems, and retail inventory management systems. Participants expressed strongly held opinions about the social appropriateness of a range of RFID applications, and were remarkably uniform in their opinions. This uniformity was especially notable when discussing the implications of in-body RFID tagging. In general, implantable chipping in humans was described as "f***ing gross," "repulsive," "invasive," "big brother watching you," "something that Hitler would have done," and "dehumanizing." Said one participant:

> P24: There's a big part of me that has a big, mmm, real question about that… you feel like you're just a bunch of robots running around, walking around.

> P24: [again, on discussing the possibility of putting RFID into humans in various scenarios] I feel like I'm turning everybody into something you can just pull off the shelf or pull out of drawer, here they are, number so-and-so.

Paradoxically, though, most participants reported that it could be acceptable, and perhaps even positive, for someone *else* to have an RFID implant. These cases generally concerned vulnerable populations such as elderly people with dementia, children, or people with severe medical allergies, but never themselves. Orientation toward RFID served as means for categorizing the "other" in society—those who should be chipped, and those who should not be chipped. Interestingly, the study participants we spoke to who told us that they had severe medical problems (for instance, conditions such as epilepsy, food allergies, or diabetes) were averse to having themselves chipped. Only one study participant (P21) held the view that embedding RFID microchips into all people is desirable. This person described implanted RFID as a mechanism for law-abiding citizens to prove they were not involved with crimes, and also envisioned RFID implantation as act of love and caring, telling the interviewer that one should "chip them [people and pets] if you loved them." Yet even this participant expressed concerns about who could gain access to information stored on implanted RFID microchips, a point we return to in the next section.

Most participants had no concerns about involuntary chipping of dangerous criminals; they associated human RFID implantation with a loss of freedom, and a rightful consequence of criminal actions:

> P10: I think they should tag like criminals, you know, that have been child molesters. But not like normal people.

In general, participants found RFID tagging of objects an acceptable use of the technology, as long as those tags were perceived as being used to track the *objects* themselves, not to monitor their *owners*. UK participants, in particular, found the idea of using RFID tags on objects to monitor their owners to be distasteful, and that this application was indicative of a "nanny state"—a government overly involved in the affairs of its citizens.

Our participants discussed a range of concerns about how systems using RFID might detract from societal values. In particular, several participants noted that they were concerned that RFID systems, such as those envisioned for automating grocery store transactions, would have the potential to detract from everyday interactions with people and undermine a sense of community.

Similarly, P26, one of the UK participants, was concerned that Oyster Card, the RFID-based fare card for London Underground transit, was unfair to people who were not knowledgeable about the public transportation system, e.g. tourists.

> P26: The way they've worked it is ...its good if you live in this country. It's cheaper. To get onto a bus on your own without an Oyster Card is about two pounds. If you get on the bus with an Oyster Card it's one pound, so it's half the fare. The only slight problem is that it's not actually fair to tourists and visitors (laughs)... basically you're ripping people off.... if you're here for a couple of weeks are you actually going to go out and get yourself an Oyster Card?

Personal and Group Identity

Some participants were reflective about media coverage and controversy surrounding RFID. They implicitly noted that concerns about the technology's use were strongly intertwined with notions of group identity, particularly with groups with which they did *not* want to be associated. For example, some participants took care to note that they were not concerned about the technology, because worrying about RFID was for people unlike them, including "religious wackos," "paranoid people," and "goody-two-shoes people who interfere with everything and know nothing half the time." Despite these claims that worrying about RFID was for people unlike them, even the most adamantly unworried participants described a number of concerns around the technology and systems using it throughout the interview.

Some participants also noted that they would not raise concerns about RFID because they saw themselves as people who actively chose not to discuss things they do not understand:

> P12: I'm not the type of person who talks about anything if I don't know about it, so I mean… I just pretty much keep moving and I don't really, I haven't really asked questions as yet.

Even though they did not fully understand the technology, however, they still noted concerns to the researchers throughout the interview; outside of the interview setting, however, they would not want to voice their opinions about the technology to a public audience.

System Trust and Data Protection

Participants expressed concerns of system trust—that is, would the technology be accurate in applications, or would it cause more trouble than it is worth? [14] Said P13, discussing the use of RFID in grocery stores:

> P13: I would be concerned if I were buying something in a grocery store about whether it worked right. Because I take things and put them in my cart and sometimes I put them back… (laughs) as my impulses change about what I want to buy. So I think if it's done wrong mistakes get made… so I wouldn't want to end up leaving the grocery store without having a final say on what my charge was, you know. Like if they charge me a hundred dollars for a gallon of milk or whatever. Um…because I think things can be programmed wrong.

Participants questioned who could gain access to data, reflecting the fact that data sharing policies are not obvious with RFID: How is data protected? Who has access? Who would want access? Who *should* have access? Where is the data going and why? A number of these concerns are a direct result of the invisibility of RFID in use, and the inability of users to determine when information is read, or even what information is read.

> P21: It just worries me where you're gonna be able to read these things. I don't mind the chip… it's where does the information go?

> P16: I don't want any information that is any way accessible to me [shared without my consent]... I want to give the information and have full knowledge of it. So any information about me I don't want stored on any device. Is that clear? I feel pretty strongly about that, because someone could steal the information and I would never know it.

> P13: For medical records and stuff I would be concerned about privacy. Because I wouldn't know, if I couldn't identify who had a scanner? I wouldn't want random people…without my permission being able to access my medical records.

When queried as to which people or organizations would want access to one's data, common responses were "the government," "people with money," "marketers chasing their demographics," "criminals," and "pocket protector people" (also described as "anyone with a brain for computers" and "hackers"). All were abstract groups, and—with the exception of marketers—no participants provided specific situations clarifying why these groups might really want access to data stored or communicated by RFID systems. Regardless, participants did not feel comfortable with these abstract groups having access to personal data.

Overall, people were concerned with not only how a technology was implemented, but also the trustworthiness of the organization deploying the technology, also known as institutional trust [14].

> Interviewer: So, how do you know if the data on a tag is accurate or not?

> P6: I guess it depends on the credibility of the companies doing… putting in the information. I'd look at their credentials, just to see how often they updated, or whatever's included in the purchase contract of the RFID tag.

These comments reflect and confirm users' concerns over data protection, a topic that has already been explored by a number of researchers in the ubicomp community

Consumer Choice and Activism

Many people clearly articulated opinions related to RFID and consumer choice—that is, they supported RFID applications in which people opted in, but not ones where people were forced in. Two separate participants discussing the difference between a shopping loyalty card and an RFID tag:

> P21: [RFID is] more risky. Because the other one is, the chip won't be a choice because, but if you put it into newborns it won't be a choice but a card, carrying a card is a choice.

> P14: I think there may be a little bit more, ah, exposure with this technology [RFID] compared to GPS. I mean, with GPS if you turn it

on it knows where you are, but if you don't turn it on it doesn't know where you are. Also if you turn on GPS it just tracks your location, it doesn't track who it is or what it is.

Despite having sophisticated understandings—and preferences—regarding being able opt-in to RFID-based systems, when asked about steps they could take to either control access to their data or correct erroneous information, participants reported feeling powerless and lacking recourse. In a general reflection on RFID deployments, one participant noted:

P22: These chips are gonna become more and more part of our lifestyle. I don't think we can stop it, but I think in some ways we're gonna lose some personal freedoms with the chip, because of the chip.

When discussing RFID passports, an American participant described the process of opting out to be fruitless:

P4: I mean maybe you could ask for one of the old ones [passports], but I don't think they would give you one, so it's kind of just out of my hands. They force you to do it

Actions to take privacy into their own hands, for example, to prevent data access by disabling RFID tags on government documents, was viewed in both countries as "more hassle than it's worth," particularly due to anti-terrorism legislation and participants' perceptions of the overall political climate.

Interviewer: Do you think there are steps you could take to stop your things from being read?

P2: Well, you can take the chip out of a dollar bill if you really wanted to and I'm sure you can probably root around in the passport and find it if that was important to you. But I don't know why you would do that because it would cause you nothing but trouble in the airport (laugh) and there's enough trouble there already.

For items tagged by non-governmental entities, people expressed disenfranchisement, noting that they did not know where to voice their access concerns:

P6: I'm very cautious with my credit cards and my personal information and things like that… in something like that [RFID] I'd be worried that it would get in the wrong hands, or get out of control, and um, you know, not knowing where to go to correct the problem, if there were to be a problem.

Some also noted that the legal system provided them no realistic options. P16, who was an attorney—and arguably a participant who would be mostly capable of navigating the US legal system—noted:

P16: If you could actually prove that the information was stolen, you could actually, you could file a claim. But you could never do that....It would always be too expensive....or too challenging.

Overall, our study participants showed concerns about RFID, yet *not a single participant* felt empowered to raise questions or otherwise challenge how the technology might be used in real-world deployments.

DISCUSSION

Our study results suggest that the way users understand how a technology works plays a crucial role in whether they deem that technology useful and how they incorporate it into their daily lives. In considering areas for continued research in ubiquitous computing, studying folk theories users hold about ubicomp systems, and studying ways to understand and design for values is fundamental to building ubiquitous technologies that inspire confidence and possess recognizable utility.

Folk Theories

In the context of RFID, our study shows that people are confused about how the technology functions. Despite this confusion, our participants held folk theories about RFID that helped them to reason about the uses and capabilities of this technology. For RFID and similar systems, studying the public's understandings of how a technology functions is an important area for continued research, since these folk theories can have profound impacts on how people orient toward ubiquitous computing technologies. For example, flawed understandings can lead to incorrect assumptions about the risks of adopting a particular technology, misplaced expectations about the benefits of a technology, and poor coping strategies when problems with the technology arise. These problems may not always have technical solutions—even if we can provide technical mechanisms to address privacy (as an example), if people's incorrect models about the technology do not account for these mechanisms they may still reject it.

Using these incorrect models to reason about RFID can, in some cases, make people uncomfortable in adopting or using the technology, even in cases where such fears may be unwarranted. For example, a user holding the "RFID as location tracking" folk theory may have (perhaps alarmist) concerns that marketers or government agencies are using RFID-based technologies to spy on him or her. These misunderstandings can have serious implications for the success or failure of a technology, and thus must be taken seriously during the design process.

Similarly, and much like other domains of technology such as e-commerce, our results show that people are concerned with trust and accuracy of the technology. How can we help provide people with an *appropriate* level of trust in the technology, especially in situations in which the technology itself is effectively invisible? This need for intelligibility of the inner workings of the technology, rather than simply keeping it invisible, echoes Chalmers et al.'s work on "seamful design" [4] as well as Dourish and Button's notion of technology that provides "accounts" of its functioning to users [5].

Additionally, beyond folk theories, there is a wide-open space to study end-user values and expectations surrounding ubiquitous computing deployments. Our results show that people use pop culture portrayals of future technologies—such as those in dystopian movies—to come to understand real-world technologies. Although the ubiquitous computing community is not in the business of movie making, we do need to consider that popular culture can and does impact how people orient toward the systems we make.

Understanding and Designing for Values

Through understanding public perceptions of emerging technologies, we as researchers and designers can begin to unpack shared societal values—for instance, about who should or should not have RFID chips implanted in them, or how RFID should be used to promote values such as fairness or community. Only once we have understood these values can we begin to consider how to design to support them, or potentially even breach them. Such understandings may be even more essential when designing for cultures that are less familiar to us.

Spiekermann and Pallas [31] have noted that technology paternalism—that is, designs in which the designer's notion of how a technology should and should not be used trumps users' own desires, or ability to appropriate the technology in their own way—is a particular danger when designing and deploying ubiquitous computing technologies. Our study participants reflected a similar sentiment; ultimately they were concerned about their own autonomy and control in the face of an ill-understood and effectively invisible technology. Yet despite such concerns, our participants were generally unwilling to publicly raise concerns about the technology or its deployments. For some, raising concerns was deeply intertwined with social identity. For others, any desire to raise concerns was compromised by a sense of hopelessness and inevitability; they doubted their ability to have a say in technology. These results raise important questions about the social implications of ubiquitous computing technologies, as well as how we might engage potential users as stakeholders in policy debates. How can system designers ensure that they are supporting end-users as stakeholders if end-users, though unhappy, refuse to speak up?

In particular, participants viewed government-backed systems as ones about which they could complain the least. They did *not* believe they had the opportunity to become partners in the design of public systems, nor did they think that their concerns would be addressed. Given that our participants were residents of two nations that view themselves as exemplars of democracy, these results are concerning. Should ubiquitous computing designers be concerned with the political context in which their systems are deployed? Again, how can we ensure that the public is empowered to participate in the design of systems that are, presumably, *for* the public?

CONCLUSION

Decisions that ubiquitous computing system designers make may have profound social implications. While performance and usability are important considerations when developing technologies, designers need to consider non-functional aspects as well. In this paper we have used a method from public policy research to facilitate users' articulation of these perspectives around RFID technology. Our findings illustrate the wide range of conceptions and beliefs that surround this technology, including the folk theories that people may use to organize accounts of RFID, perceptions of appropriateness in a range of application contexts, and the ways in which interpretations of social meaning may impact ones' willingness to express concerns around the technology. Understanding these factors that affect—and can even determine—how or whether users will adopt a technology becomes even more essential as ubicomp moves out of the lab and moves into the world.

ACKNOWLEDGMENTS

Thanks to Alex Taylor, Tom Rodden, and Jeonghwa Yang for recruiting study participants, and Jennifer Stoll for helpful advice during data analysis. This work was supported by grants from Cisco and the National Science Foundation (NSF-CNS #0626281), and graduate research fellowships from the US Department of Homeland Security and the National Science Foundation.

REFERENCES

[1] Beckwith, R. Designing for Ubiquity: The Perception of Privacy. *IEEE Pervasive Computing*, 2003, 40-46.

[2] Bijker, W.E. *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. MIT Press, Cambridge, MA, 1995.

[3] Cardullo, M.W. and Parks, W.L. Transponder Apparatus and System. United States Patent, 1973.

[4] Chalmers, M., Dieberger, A., Höök, K. and Rudström, Å. Social Navigation and Seamful Design. *Cognitive Studies*, *11*, 3 (2004), 1-11.

[5] Dourish, P. and Button, G. On "Techno-methodology": Foundational Relationships between Ethnomethodology and System Design. *Human-Computer Interaction*, *13*, 4 (1998), 394-432.

[6] Dourish, P., Grinter, R.E., Delgado de la, F., Jessica and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Computing*, *8*, 6 (2004), 391-401.

[7] Du Gay, P., Hall, S., Janes, L., Mackay, H. and Negus, K. *Doing Cultural Studies: The Story of the Sony Walkman*. Sage Publications, 1997.

[8] Egenhofer, M.J. and Mark, D.M. Naive Geography. *Spatial Information Theory—A Theoretical Basis for GIS, International Conference COSIT*, *95* (1995), 1-15.

[9] Floerkemeier, C., Schneider, R. and Langheinrich, M. Scanning with a Purpose: Supporting the Fair information Principles in RFID Protocols. *2nd International Symposium on Ubiquitous Computing Systems (UCS 2004)*, 2004, 214-231.

[10] Friedman, B., Hurley, D., Howe, D.C., Felten, E. and Nissenbaum, H. Users' Conceptions of Web Security: A Comparative Study. *ACM CHI 2002*, 2002, 746-747.

[11] Friedman, B., Kahn, P.H. and Borning, A. Value Sensitive Design and Information Systems.

Human-Computer Interaction and Management Information Systems: Foundations, New York, 2006, 348-372.

[12] Gaw, S., Felton, E.W. and Fernanadez-Kelly, P., Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail. *ACM CHI 2006*, 2006, 591-600.

[13] Goffman, I. *The Presentation of Self in Everyday Life*. Doubleday, Garden City, New York, USA, 1959.

[14] Grabner-Kräuter, S. and Kaluscha, E.A. Empirical Research in On-line Trust: A Review and Critical Assessment. *International Journal of Human-Computer Studies*, *58*, 6 (2003), 783-812.

[15] Günther, O. and Spiekermann, S. RFID and the Perception of Control: The Consumer's View. *Communications of the ACM*, *48*, 9 (2005), 73-76.

[16] Hall, S. *Representation: Cultural Representations and Signifying Practices*. Sage Publications, 1997.

[17] Hayes, P.J. The naive physics manifesto. *Expert Systems in the Micro-Electronic Age (*1979), 242–270.

[18] Hendry, D.G., Sketching with Conceptual Metaphors to Explain Computational Processes. In *Proc. IEEE VL/HCC 2006,* 2006, 95-102.

[19] Juels, A. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, *24*, 2 (2006), 381-394.

[20] Kempton, W. Two Theories of Home Heat Control. *Cognitive Science*, *10* (1986), 75-90.

[21] Kriplean, T., Welbourne, E., Khoussainova, N., Rastogi, V., Balazinska, M., Borriello, G., Kohno, T. and Suciu, D. Physical Access Control for Captured RFID Data. *IEEE Pervasive Computing*, *6*, 4 (2007), 48-55.

[22] Langheinrich, M. Privacy By Design: Principles of Privacy-Aware Ubiquitous Systems *Ubicomp 2001*, 2001, 273-291.

[23] Langheinrich, M. RFID and Privacy. *Security, Privacy, and Trust in Modern Data Management*, Springer, New York, 2007.

[24] Mäkelä, K., Belt, S., Greenblatt, D. and Häkkilä, J. Mobile Interaction with Visual and RFID Tags: A Field Study on User Perceptions. *ACM CHI 2007*, 2007, 991-994.

[25] Morgan, M.G., Fischhoff, B., Bostrom, A. and Atman, C.J. *Risk Communication: A Mental Models Approach*. Cambridge University Press, New York, 2002.

[26] Morton, S. Barcelona Clubbers Get Chipped. *BBC News*, 2004.

[27] Nathan, L.P., Friedman, B., Klasnja, P., Kane, S.K. and Miller, J.K. Envisioning Systemic Effects on Persons and Society Throughout Interactive System Design *ACM DIS 2008*, 2008.

[28] Orlikowski, W.J. and Gash, D.C. Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems*, *12*, 2 (1993), 174-207.

[29] Poole, E.S., Chetty, M., Grinter, R.E. and Edwards, W.K. More Than Meets the Eye: Transforming the User Experience of Home Network Management. *ACM DIS 2008*, 2008.

[30] Rothensee, M. and Spiekermann, S. Between Extreme Rejection and Cautious Acceptance: Consumers' Reactions to RFID-Based IS in Retail. *Social Science Computer Review*, *2008*, 26 (2008), 75-86.

[31] Spiekermann, S. and Pallas, F. Technology Paternalism: Wider Implications of Ubiquitous Computing. *International Journal of Technology Assessment and Ethics of Science*, *4*, 1 (2006), 1615-6609.

[32] US Department of State.. Electronic Passports. http://travel.state.gov/passport/

[33] Verichip. http://www.verichipcorp.com.

[34] Voida, A., Grinter, R.E., Ducheneaut, N., Edwards, W.K. and Newman, M.W. Listening in: practices surrounding iTunes music sharing *ACM CHI 2005*, 2005, 191-200.

[35] Vosniadou, S. and Brewer, W.F. Mental Models of the Earth: A Study of Conceptual Change in Childhood. *Cognitive Psychology*, *24* (1992), 535-585.

[36] Want, R. *RFID Explained: A Primer on Radio Frequency Identification Technologies*. Morgan & Claypool, 2006.

[37] Whitten, A. and Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 *8th USENIX Security Symposium*, 1999.

[38] Yan, Z. What Influences Children's and Adolescents' Understanding of the Complexity of the Internet? *Developmental Psychology*, *42*, 3 (2006), 418-428.