An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies

David H. Nguyen, Alfred Kobsa, Gillian R. Hayes
Department of Informatics
Donald Bren School of Information and Computer Sciences
University of California, Irvine
{dhn, kobsa, gillianrh}@ics.uci.edu

ABSTRACT
This paper presents an exploration and analysis of attitudes towards everyday tracking and recording technologies (*e.g.,* credit cards, store loyalty cards, store video cameras). Interview participants reported being highly concerned with *information privacy*. At the same time, however, they also reported being significantly less concerned regarding the use of everyday technologies that have the capabilities to collect, process, and disseminate personal information. We present results from this study that both identify and begin to explain this discrepancy.

Author Keywords
Tracking, recording, privacy, everyday technologies, retail, user study.

ACM Classification Keywords
K.4.2 [Computers and Society]: Social Issues; K.8.m [Personal Computing]: Miscellaneous

INTRODUCTION

Two common research themes in Ubiquitous Computing are automated capture and access [26] and context-aware computing [21]. Their application spans a variety of domains including education [4][8], healthcare [2], interpersonal relationships [5][18], personalization [17], and automation [28]. These applications require the tracking and recording of large amounts of domain and problem-specific data about individuals and their surroundings, a situation that inherently engenders concerns about the use, re-use, control, protection, and potential abuse of those data. Although tracking and recording technologies greatly advance these research areas, they may also invoke a variety of privacy-related concerns.

Thus, researchers in Ubicomp have investigated many privacy-related issues and concerns surrounding tracking and recording technologies. These investigations have often uncovered generalized concerns about the tracking and recording that is inherent in Ubicomp systems (*e.g.,* [2], [11], [25]). At the same time, however, other investigations have indicated that people are not concerned with many new Ubicomp technologies (*e.g.,* [5], [20]). This work focuses on specific concerns regarding specific technologies in the concrete context of everyday retail and financial transactions. Extending beyond general concerns, the results presented from this work uncover current attitudes towards everyday tracking and recording technologies. This work contributes insights into attitudes around these technologies that may support the design, deployment, and adoption of new technologies.

In this paper, we describe the results of a user study focused on attitudes and concerns surrounding everyday tracking and recording technologies. Specifically, we studied attitudes towards credit cards, store loyalty cards, electronic toll collection systems, web server records, store video cameras, and radio frequency identification (RFID). These technologies by no means include every tracking and recording device; they were chosen because they are mostly well known and represent a broad sampling of technological capability and contextual use. This research focuses on how attitudes in specific contexts with regard to specific technologies may or may not relate to or depend upon general *information privacy*[1] concerns.

Participants in this study reported high levels of information privacy concerns but much lower levels of concern for tracking and recording technologies in retail transactions and in other everyday activities (concerns about RFID which is a novel technology were comparatively higher). The results presented in this paper identify and begin to explain this discrepancy.

METHOD

We used a mixed-method approach to study the experiences of U.S. consumers with a variety of everyday tracking and recording technologies. This approach included the use of a questionnaire to gauge their attitudes, and a follow-up interview focused on their rationales for those attitudes. We

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

[1] Information privacy refers to "the ability of the individual to personally control information about one's self" [22].

surveyed seven sites in two distinct geographical areas in the United States to sample a broad variety of consumers.

Participation in the study was initially framed as an inquiry into consumer attitudes towards a relatively novel Ubicomp technology in the retail space - RFID. That is to say, participants were provided study descriptions that focused on RFID but questionnaires that covered a variety of everyday tracking and recording technologies. This approach allowed us to poll participants' attitudes surrounding information privacy, data collection, data control and data use around a wide variety of technologies without biasing them towards specific concerns by using potentially loaded terms like privacy and surveillance.

Participants

Fifty-four participants (27 female, 27 male) were recruited at seven sites. To include a broad variety of respondents, recruitment was done at a variety of shopping malls in two primary geographic areas:

(A) a high-end[2] outdoor mall, a midrange[3] outdoor mall, and three midrange indoor malls in Southern California (n=18), and

(B) a midrange indoor mall and a midrange shopping center in Southern Louisiana (n=36).

Participants represented a wide range of demographic profiles. They were nearly evenly divided into three age groups: 18 to 29, 30 to 50, and over 51. Slightly over half of the participants reported being married or in a domestic partnership (58%); 33% were single; and 9% were separated, divorced or widowed. The highest level of education achieved for most participants was a high school degree (59%), but 15% were college graduates with 24% having at least some graduate school education or having completed a graduate degree. Individual income levels were again nearly evenly divided across three intervals: less than 30,000 USD a year; between 30,000 and 60,000 USD; and over 60,000 USD. We present these demographics primarily to indicate the variety of study participants but also later highlight those results that appear to be correlated in some way to this demographic information.

Recruitment

Participants were recruited by a single researcher in public sitting areas and "food courts" at each site. Systematically approaching everyone in the chosen area, the researcher invited every adult (over 18 years of age) to participate in the research study. When every potential participant in the sitting area or food court had been approached, the researcher walked to a different end of the mall, again systematically approaching shoppers. When people declined to answer the survey and participate in the interview on site, a flyer was distributed with contact information to participate at a later time. Areas within each site were alternated in this manner for every site visit, each of which typically lasted three to four hours.

In addition to direct recruitment at these sites (n=36), snowball sampling was also used – asking participants to advertize the study to others in their social circles who might be interested in participating (n=18). For the convenience of the participants, both those directly recruited and those recruited through social networks, the survey was also conducted at people's homes and places of work (coincidentally, n=18). However, for safety and to provide a context of shopping in which many of these everyday tracking and recording technologies are currently used, participants were encouraged to complete the study at the mall. Participants each received a $10 gift card as compensation for their time.

Procedure

When a person agreed to participate, the researcher first asked the participant about any prior knowledge of RFID or its applications. Prior knowledge was documented, but regardless of any prior knowledge every participant was then shown a diagram of the usage of RFID [28], presented with sample RFID tags, and given a short presentation to introduce and explain RFID. Participants were then given the opportunity to ask any questions about RFID until they felt comfortable with their understanding of the technology and its uses. Once all questions had been answered, participants completed a pen and paper questionnaire of 116 questions. The researcher then conducted a semi-structured interview using the questionnaire as a guide but allowing the participant to lead the discussion to topics of individual interest. The entire process took approximately 45-60 minutes.

Survey Apparatus

The survey included four primary sections: one dedicated to RFID, one focused on information privacy, one focused on other everyday tracking and recording technologies, and one for demographic data.

The section dedicated to RFID included Boslau's questionnaire design [3]. Additional questions focused on the desirability of potential benefits as well as comfort level with potential tracking of people and their items by thieves, strangers, companies, and the government.

The second section contained the Smith *et al.* privacy instrument [22]. This instrument is a parsimonious questionnaire consisting of 15 questions. This section was included to allow for a comparison of the participants in our study with those in Smith *et al.* regarding their attitudes towards information privacy. This instrument divides information privacy into four subscales of concern:

[2] We define high-end malls as malls that contain boutiques and stores that cater to designer brands. These malls have full-service restaurants.

[3] We define midrange malls as focused on ready to wear brands with a mix of "food court" and full service restaurants. For the sake of completeness, low-end malls emphasize discounts over service and branding.

collection, errors, unauthorized secondary use, and improper access. The c*ollection* subscale measures the concern that extensive amounts of personally identifiable data are being collected and stored in databases. *Errors* measures the concern that protections against deliberate and accidental errors in personal data are inadequate. *Unauthorized secondary use* measures the concern that information is collected for one purpose but used for another. *Improper access* measures the concern that data about individuals are readily available to people not properly authorized to view or work with this data. And finally, the *overall* scale is the average of all questions that make up the above four subscales.

The third section included questions about a series of everyday tracking and recording technologies to gauge attitudes and concerns regarding these technologies. The technologies included credit cards, store loyalty cards, electronic toll collection systems, web server records, and store video cameras.

Finally, the fourth section included questions focused on demographic data. These questions included gender, age, marital status, number of children, cultural background, ethnicity, income, educational background, and profession. These questions were intentionally left to the last section so as to minimize any potential impacts reflecting on demographic data may have on responses.

Analysis

One researcher took multiple passes through the data using open coding to determine 26 codes. Once that coding scheme was identified, the researcher then used axial coding to determine links between them to create themes, building a model for how participants encounter and understand everyday recording technologies.

We also conducted a comparative quantitative data analysis, but were limited by the data reported by Smith *et al.* who only reported means, standard deviations, and numbers of participants in their study. We were only able to perform t-tests with the published data in comparison with the discrete data gathered in this study. Thus we present any observed differences between the results of the studies as only potentially significant.

RESULTS

Participants were queried about six tracking and recording technologies: credit cards, store loyalty cards, electronic toll collection systems, web server records, store video cameras, and RFID. With the exception of RFID and electronic toll collection systems (which is an active RFID system), most participants had used or experienced all these technologies for multiple years. Most participants declared themselves to be familiar with electronic toll collecting systems (n=43), but very few had installed them in their cars (n=10). Even few participants were familiar with RFID (n=7). These numbers confirm that RFID is a *novel* technology. We categorize the other five technologies (including electronic toll collection) as *everyday* technologies.

In this section, we report quantitative results indicating participants' levels of concern towards information privacy, and towards everyday tracking and recording technologies. Thereafter, we present results from our interviews that explain some of the observations from the numerical data.

Privacy Subscale	**μ (σ) this study (n = 54)**	**μ (σ) Smith *et al.* study #1 (n = 146)**	**μ (σ) Smith *et al.* study #2 (n = 183)**	**μ (σ) Smith *et al.* study #3 (n = 337)**
		t-test with this study	**t-test with this study**	**t-test with this study**
Collection	5.39 (1.21)	5.28 (1.19)	5.11 (1.04)	5.45 (1.16)
		p = 0.564 t = 0.578 df = 198	t = 0.096 1.673 df = 235	p = 0.726 t = 0.351 df = 389
Errors	5.68 (0.90)	5.36 (1.06)	5.57 (0.99)	5.46 (1.11)
		p = 0.050 t = 1.970 df = 198	p = 0.465 t = 0.732 df = 235	p = 0.167 t = 1.385 df = 389
Unauthorized Secondary Use	6.54 (0.65)	5.77 (1.22)	5.74 (1.14)	6.15 (1.07)
		p = 0.001 t = 4.408 df = 198	**p = 0.001** t = 4.921 df = 235	**p = 0.010** t = 2.6009 df = 389
Improper Access	6.40 (0.63)	6.10 (0.89)	5.83 (1.01)	5.90 (1.01)
		p = 0.024 t = 2.274 df = 198	**p = 0.001** t = 3.925 df = 235	**p = 0.001** t = 3.527 df = 389
Overall	6.00 (0.59)	5.63 (0.78)	5.56 (0.83)	5.74 (0.86)
		p = 0.002 t = 3.165 df = 198	**p = 0.001** t = 3.632 df = 235	**p = 0.033** t = 2.141 df = 389

Table 1: Comparison of Levels of Concern on a 7-point Likert scale (higher values indicate higher concern)

Attitudes Towards Information Privacy

The participants in this study reported similar or even higher levels of concern towards information privacy than those measured by Smith *et al.* [22], using the same privacy instrument as those authors. Table 1 shows the comparison between the average level of concern reported by the participants of in this study and the average of the Smith *et al.* studies [22] reported in 1996. The three right columns list the results of a two-tailed unmatched t-test between the participants of this study and the population measured by Smith *et al.* P-values, t-values, and degrees of freedom are provided. Significant p-values (< 0.05) are shown in bold. With respect to the 'overall' privacy scale, participants reported significantly higher levels of concern for information privacy than the levels found in the previous three Smith *et al.* studies.

Within the demographics of the subject population, the only significant differences uncovered were in the 'overall' scale with respect to location ($t(52) = 1.7811$, $p < 0.05$, one-tailed t-test) and gender ($t(52) = 2.5037$, $p < 0.01$, one-tailed t-test). That is, participants in California reported being more concerned than participants in Louisiana, and female participants reported being more concerned than their male counterparts. Interaction effects could also be observed. Across all subscales, women in California reported being significantly more concerned than their male counterparts: collection ($t(16) = 1.70$, $p < 0.05$), errors ($t(16) = 5.73$, $p < 10^{-6}$), unauthorized secondary use ($t(16) = 1.80$, $p < 0.05$), improper access ($t(16) = 2.53$, $p < 0.05$), and especially overall ($t(16) = 5.18$, $p < 10^{-6}$), all one-tail t-tests. In contrast, there were no significant differences in gender for the Louisiana population.

Technology	μ (σ) n
Credit card "I am concerned that my credit card purchases are recorded."	3.65 (1.71) n = 52
Store loyalty cards "I am concerned that my purchases at stores can be tracked when I use their loyalty card."	3.47 (1.71) n = 49
Electronic toll collection "I am concerned that the electronic toll collection system has a record of my trips on the toll roads."	2.93 (1.68) n = 43
Web server records "I am concerned that websites have a record of my activities when I visit them."	4.43 (1.90) n = 53
Store video cameras "I am concerned about the surveillance cameras in stores."	2.85 (1.87) n = 54

Table 2: Concern for Everyday Technologies on a 7-point Likert Scale (higher values indicate higher concern)

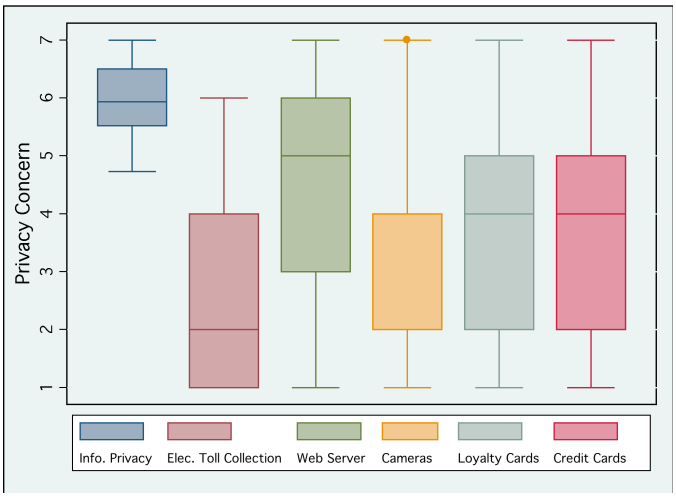

Figure 1: Information Privacy Concerns vs. Everyday Tracking Technologies Concerns (higher values indicate higher concern)

Attitudes Towards Everyday Tracking and Recording Technologies

Participants rated their levels of concern with the five studied everyday tracking and recording technologies. Ratings were given regarding concerns about each technology on a seven-point Likert scale ranging from "strongly agree" (7) to "strongly disagree" (1). The wording and numeric results can be found in Table 2. With the exception of web server records ($\mu = 4.43$, $\sigma = 1.90$), participants reported low levels of concern (less than 4) for the records kept by everyday technologies that were studied.

These levels of concern are strikingly lower than the levels of concerns reported when participants were asked about information privacy (see Figure 1). Figure 1 shows the box plots[4] of concerns for the five studied everyday tracking and recording technologies. It also shows the concerns for information privacy, which is the *Smith et al.* 'overall' scale. From this figure, a discrepancy can be seen between the stated generalized information privacy concerns and the stated concerns for some everyday tracking and recording technologies.

[4] A box plot, also known as a box and whisker diagram, represents graphically the five-number summary of a data set. The line in the middle of the box is the median. The edges of the box are the lower and upper quartiles. The whisker parts of the diagram are typically the minimum and maximum values. "Outliers" are represented as dots. [29]

Attitudes towards RFID

Our results indicate that RFID is relatively unknown within this subject group. Of the 54 participants, only 7 participants (13%) reported knowing anything about RFID previously. This percentage is comparable to the two Spiekermann studies, in which 14% and 19% had heard of RFID previously [25], but is low in comparison with the 23% of U.S. participants who reported being knowledgeable with RFID in a Capgemini study [6] or the 38% of U.S. participants in the Queen's University international survey on surveillance and privacy [30].

When asked to weigh the potential benefits of RFID to its potential costs, the majority of participants responded that the potential benefits outweigh the potential costs (70%, 38 out of 54) with $\mu = 5.11$, $\sigma = 1.91$, where "strongly agree" is 7 and "strongly disagree" is 1. The remaining participants were divided evenly between being neutral (15%, 8 out of 54) and reporting that costs outweigh benefits (15%, 8 out of 54).

The questionnaire also included questions about concerns about tracking through RFID by four different entities: strangers, the government, thieves, and companies. For each entity, the questionnaire included a question about three different aspects of tracking: "[entity] finding out what RFID-tagged items I buy," "[entity] finding out what RFID-tagged items I wear or carry," and "[entity] tracking where I and my RFID-tagged items go." The results of the three questions are averaged for each entity to produce a level of concern for each entity (see Table 3 and Figure 2). Figure 2 shows the box plots of concerns for the tracking of RFID by strangers, government, thieves, and companies. It also shows the concerns for information privacy, which is the *Smith et al.* 'overall' scale. From this figure, it seems the stated information privacy concerns and the stated concerns for tracking by RFID are more aligned than the stated concerns of everyday tracking technologies seen in Figure 1. It is interesting to note that despite the high level of concern reported for tracking by RFID, when asked to weigh the potential advantages and the potential disadvantages of RFID, the majority of participants reported favoring the potential advantages.

RFID Tracking by	μ (σ)
Strangers	5.18 (1.43)
Government	4.91 (1.79)
Thieves	5.45 (1.55)
Companies	4.50 (1.67)

Table 3: Concern for RFID Tracking on a 7-point Likert Scale (higher values indicate higher concern)

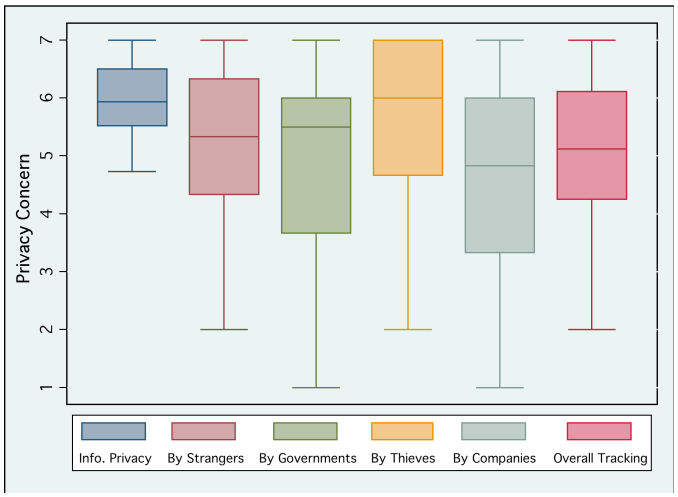

Figure 2: Information Privacy Concerns vs. RFID Tracking Concerns (higher values indicate higher concern)

Comfort with Recording and Tracking Technologies

Three themes surrounding comfort with everyday recording and tracking technologies were identified in the interviews with study participants:

1. Threat comprehension
2. Expectations of privacy
3. Situational dynamics

In this section, we describe each of these themes and present evidence that demonstrates their impact on the attitudes of interview participants.

Threat Comprehension

Participants reported a clear understanding of potential benefits of recording and tracking technologies. For example, participants commented on the ease of use of credit cards. At the same time, they had difficulties articulating possible costs or threats of these technologies. For example, participants often struggled to describe any problems with credit card records, and when pressed would comment on identity theft, credit card abuse and so on, never mentioning the potential for building long-term records of their purchases or other threats commonly discussed in the discourse on privacy and consumer technologies [14]. Several participants also commented that they had not spent much time thinking about how such records could negatively affect them. For example, when asked about web sites recording visits, one participant commented: "I've never given it a single thought. I mean, I've known about it…But yes, it just it's never been a concern." Likewise, when asked how data tracked through store loyalty cards might be used, another participant commented: "I've actually never thought of that."

Of those who had given the records previous consideration, a common response was that such records were irrelevant or harmless. For example, when asked about the records produced through store loyalty cards, one participant commented:

You mean how much coffee I drink? That's relatively harmless I think. Some information can be harmless. Some can be detrimental, depending on how it's used. Knowing how many coffees I buy, I don't see a problem with that personally.

Records were often reported to be benefits, rather than risks or costs. A credit card record could be proof that an actual purchase was made. Electronic toll collection records could be a possible alibi. Otherwise, recording and tracking of everyday activities were often reported to be irrelevant or harmless. Commenting on credit card records, a participant said:

Well, personally I don't think it affects me negatively in any way. But if somebody would take my card or steal it and use it to get funds off of there, then it would be very helpful to have that information so that I could get it back.

Despite struggling to articulate the potential costs and risks, participants did often present the impression that they *should* be concerned. As one participant commented, "I know I should be concerned, but I don't know why."

While some participants acknowledged that they should be concerned, others avoided thinking about the threats, despite acknowledging fear of the situation. When asked about store loyalty cards, one person reported fearing the unknown uses of that information, but did nothing to address it:

You know, I have no idea, and that scares the crap out of me. But I don't really… I don't really think about these things.

Finally, participant comments also indicated flawed mental models of the inner workings of technologies, which further contributed to their difficulty in understanding the potential threats of these technologies. For example, when queried about web server records, participants frequently commented that "hackers" could get their information, thus causing items like cookies to be of concern to them. Although hacking is a legitimate security threat, it is not one that can be created through web tracking technologies. Despite this technological impossibility, concerns about web tracking technologies were significantly more common than the typical recording technologies queried, such as electronic toll collection or pervasive video surveillance.

All but one participant reported that recording and tracking technologies were not problematic for people who are "not doing anything wrong" or have "nothing to hide." For example, in response to questions about video surveillance cameras, one participant commented that the cameras were there for: "… keeping track on the bad guys. If you're a good guy, you've got nothing to worry about."

Although this attitude is not necessarily surprising [24], it represents an important challenge in the discourse and design surrounding recording technologies as well as their evaluation. Even when people are obeying laws and "doing the right thing," they may still have secrets or wish to negotiate the boundaries of information dissemination with friends, coworkers, strangers, and even institutions [19].

Expectations of "Privacy"

The majority of participants commented that in public, particularly in shopping spaces such as the ones in which this study took place, it is unrealistic to expect any level of "privacy." Commonly deployed technologies like video surveillance cameras and closed circuit television (CCTV) were frequently viewed as pervasive but nevertheless permissible recording technologies. This result echoes some of the results of other researchers more specifically focused on CCTV [10][15][16]. This attitude was compounded when the recording technologies were included as part of a service. For example, the records created as part of the electronic toll collection were seen as an inherent part of service use.

Participants also held the belief that tracking and recording was not of great concern because problems will be taken care of by some other entity, be it the government or even some higher power. For example, when asked about fearing government oversight, one participant responded:

That doesn't bother me. Well, like I said, I believe the Bible is true, and the Bible says to support and pray for whoever is in charge of your government, whether you agree with them or not, ask God to give him the strength to make the right decisions and the wisdom to make the right decisions for all the people. And I think he has a hand in everything. So I could go crazy worrying about things all the time…

Some participants reported trusting their information to be regulated by the government. Corporations were often seen as having the highest potential to abuse the information they were collecting. When asked about the possible uses of the records, one participant commented:

I don't think it's used to help consumers; I think it's used to find consumers, to target consumers. I think very few corporations use their abilities to help consumers and they shouldn't; they're in a - it's a profit business.

When asked about the same issue, another participant was not concerned as long as:

Well as long as the corporations like had loyalty to the customers and didn't really like divulge information like unlawfully. And so, I guess as long as there's like codes and regulations making it like illegal to do so.

As exemplified by the previous quote, it was common for participants to expect the government and the law to protect them. This expectation is not unique to the participants in this study; the feeling of being protected by the law can also be seen in the Queens University survey on surveillance [30]. Of those who indicated in that survey that they are

knowledgeable of laws that protect personal information *in government departments*, 51% thought those laws were either very effective or somewhat effective. Of those who considered themselves knowledgeable of laws that protect personal information *in private companies*, 51% thought those laws were either very effective or somewhat effective (coincidentally, the percentages are identical but not the specific respondents).

Another commonly reported belief – indicating that tracking and recording is a minor issue – is that individuals would be hidden in the large databases. This deindividuation in a crowd of millions was often reported to be a protection against threats. For example, in describing comfort with web server records, one participant noted:

> *There are so many people doing it that it doesn't matter, so, that's the way you look at it. That's the way my brother described it. He's a programmer. He goes, "Who cares." Too many people. So you just get lost in the crowd.*

Situational Dynamics

General beliefs may not always coincide with beliefs in specific situations (see Figures 1 and 2). In fact, a specific goal of this study was to bridge the gulf between generalized notions of information privacy and specific behaviors by examining attitudes about specific situations, in this case everyday recording in shopping contexts. Although we still do not capture actual behaviors in this work, garnering reactions in specific contexts can be a step towards bridging that gap. The Smith *et al.* instrument [22] queries participants about information privacy in general. However, when asked about specific tracking and recording technologies, participants reported being less concerned than in the general case. Moreover, when asked about tracking via RFID, a technology that participants believed to be novel and rare and that has no specific, common usage yet, they replied with similar high levels of concern as when asked about general information privacy. This suggests that answers are dependent on the situation.

Situational context has an impact in reported attitudes – not only the context of the specific product and service but also the context of the people, institutions, places, and activities surrounding any interaction with those products and services.. For example, the participants in our study reported not to be concerned with the tracking and recording of store loyalty records. However, they reported being significantly more concerned about web server records. Without knowing the true costs and benefits, participants bring different knowledge and models into appraising a level of concern for that particular situation or technology. When asked, a participant explained his understanding of what happens with web server records:

> *It can affect it if the information that I provide is somehow pirated by someone who's not authorized to receive it. I'm concerned about the yeah, I'm concerned about pirates. I wouldn't want any pirating and take the information and use for a bad purpose because there are lots of pirates there on the Internet.*

A lack of options may be another factor in risk assessment. Participants reported using the web despite concerns of being tracked, because there were no other options if they wanted the online information or services. Participants also reported using store loyalty cards despite concerns because they could not afford not getting the discounts. So without options, people are "forced" to use a particular technology or service.

Analysis of the level of effort required alongside the level of concern and the likelihood of having an impact was also reported to influence attitudes. Participants considering circumventing tracking and recording often commented that it may not be worth the effort. For example, one participant described being concerned about the presences of cameras in hotels. When asked if that meant he would not stay at hotels with cameras, he responded: "No, it's not like I'm going to sit there and search for the only hotel in Las Vegas that doesn't have surveillance cameras."

Thus, as exemplified in this account, the discrepancy between participants' attitudes towards everyday tracking and recording technologies and their fears and concerns are grounded in three areas. First, they may not understand the collection, processing, and dissemination of recorded consumer data. Second, they may not expect "privacy," because in various ways, tracking and recording consumer data is a not a major issue. And lastly, there is a discrepancy depending on the situation, because some situations are likely to provoke more concern and action than others.

DISCUSSION

In the last decade, research in Ubicomp has investigated many privacy-related issues and concerns surrounding recording and tracking technologies. Some studies have uncovered general privacy concerns; at the same time, other investigations have indicated that people are not concerned with many new Ubicomp technologies. Far from claiming that there is a single answer to these potentially conflicting findings, the results of this study demonstrates that people can simultaneously be concerned about data tracking and recording while using these technologies and services on a regular basis.

Researchers have used a variety of arguments to reconcile the discrepancy between these two sets of research findings. Hayes *et al.* described factors that together influence people's decision making about a specific audio and video recording installation [9]. Consolvo *et al.* and others describe how people might be trading their data and information for the value provided by the product or service [7][12]. A similar argument is that if people are already using these technologies, then they have already consented to the tracking and recording that is a part of these technologies. This argument is based on the premise that people will protest if they object to new technologies, as was the case in an organized boycott of Benetton products

following the announcement of a new embedded RFID program for their clothing line[5].

Although these conceptions of the acceptance of recording and tracking in everyday life are important and useful, there still remains room for research in developing a complete model of how tracking and recording technology becomes accepted. In particular, with regard to individuals' ability to conduct the cost/benefit analyses suggested by these arguments, they must understand both the costs and the benefits of a technology. The results presented in this paper, however, indicate that this understanding in individuals is lacking in two fundamental ways:

1. Their ability to assess potential threats of what is tracked and recorded.
2. Their assessment of their capabilities and options to do anything about those threats, which would enable a negotiation of when, how, and to what extent information about them is disseminated to other parties.

Additionally, the discrepancy between general and specific concerns regarding data collection, processing, and dissemination may be caused by the nature of the questions themselves. Asking in general terms might encourage people to answer in the most conservative way. Because anything can happen in the abstract sense, people may tend to answer conservatively, in order to be on the safe side. If, on the other hand, people are asked in the context of a specific technology or activity, such as in connection with a specific Ubicomp research project, they might instead reflect on previous experience with that context. Their answers then would suggest their experiences with that context (positively or negatively). One may therefore expect that answers regarding concrete cases might be more in line with actual behavior and practices than answers to more abstract questions.

Perhaps the most important reason for the survey participants not to be worried about tracking and recording is that on a large scale, nothing blatantly harmful has happened to them yet, what Hayes *et al.* referred to as "experiential cues" [9]. Apart from isolated situations, the threats from these tracking and recording technologies remain largely hypothetical. There is no "Big Brother." Data may be collected, but there is no single central repository. With the exception of large data aggregation services, such as those provided by ChoicePoint, data about individuals is currently distributed across many different institutions, many different databases, and many "Little Brothers" [23]. And thus far, generally not much harm has come to the participants from the use or abuse of these databases. It is therefore only natural that they have not given the issue much thought, and thus their level of concern is low.

[5] http://www.boycottbenetton.com/

RELATED WORK

Many researchers worked on eliciting the privacy-related attitudes and behaviors of people and their interaction with and usage of potentially privacy-invasive technologies. A full review of these works is beyond the scope of this paper. We describe a subset of the most related studies in different areas that have noted the discrepancy between attitudes in general contexts (high concern for information privacy) and in specific contexts (low concern for actual usage with certain technologies).

Van de Garde-Perik *et al.* [27] noted the "discrepancy between stated attitudes and user behavior relating to privacy". Participants in their experiment with a music personalization application characterized personality traits as sensitive information. However, this supposedly "sensitive" information was shared in much the same extent as the claimed less-sensitive music preferences. Building on this work that analyzed only a single application, our research focuses on one novel technology and several other often-used everyday technologies and services.

In a study of the practices of web users, Jensen *et al.* [13] also reported a mismatch between self-reported user attitudes and observed user behaviors. Moreover, users did not know what to use to make privacy-related decisions about the websites. Similar to Jensen *et al.*, the participants in our study also expressed a high level of concern for information privacy. Additionally, when asked about technologies beyond the web, participants in our study also were not able to gauge the threats of the studied everyday technologies and services, in order to assess their concerns.

In the area of store loyalty cards, Consolvo *et al.* [7] noted a similar discrepancy. Users asserted a high concern for "privacy" but nevertheless used store loyalty cards. Consolvo *et al.* interviewed only two subjects for the qualitative part of their study, while this study interviewed 54 people.

In his analysis of tracking and recording technologies for eldercare, Beckwith [2] also saw these discrepancies. Specifically, the participants in that study did not understand the technology. It was effectively a black box to them. Beckwith showed that people are not capable of understanding the privacy tradeoffs of *novel technologies*. Our study shows that participants do not understand the recording capabilities of *everyday technologies* either, and therefore are also not capable of understanding the privacy tradeoffs of these technologies. Another difference is that in contrast to the short-term interaction with novel technology in the Beckwith study, our study also dealt with technologies that have been in use for multiple years.

Perhaps most relevant are Spiekermann's RFID user studies [25], in which participants were shown videos of the costs and benefits of RFID. Thereafter, participants were asked to rate their level of desire to 1) deactivate the tags at checkout, 2) keep the tags but let users control through a password what device can read the tags, or 3) keep the tags

and have a system decide, depending on previously set preferences, what device can read the tags. Participants in that study were highly concerned about RFID tags and preferred deactivating the tags at checkout.

One concern about many of these studies is that the technologies presented are very novel. Participants would most likely not have had any previous experience with the technology. Therefore, participants' attitudes are mostly based on conjecture and impulsive opinions. To compensate for this concern in our study, we asked not only about RFID, but also other tracking and recording technologies that are already being used on a daily basis. In this case, participants do not have to speculate about novel technologies, but can leverage their years of experience with these everyday technologies.

Spiekermann's study reported a greater concern for RFID than the participants of our study. One major difference between the two studies is that Spiekermann surveyed Germans while we surveyed Americans. This cultural difference may account for the differences in the reported attitudes.

CONCLUSION

This paper describes the results of a study on attitudes and understanding regarding everyday and novel tracking and recording technologies. When asked about their attitudes towards information privacy in general, participants reported being highly concerned about information privacy. However, at the same time, the very same people are significantly less concerned (and generally unconcerned) regarding the use of everyday technologies that have the capability to collect, process, and disseminate personal consumer data.

This discrepancy in attitudes has broad consequences for the deployment of new tracking and recording technologies, such as RFID. It suggests that misunderstandings and ignorance with respect to these technologies and their tracking and recording infrastructures could sway people to adopt or reject a technology. Understanding people's attitudes and perspectives regarding these everyday tracking and recording technologies may give insights into the adoption of technology with similar characteristics that is currently still novel, as well as technologies yet to be developed.

ACKOWLEDGEMENTS

A U.S. Department of Education GAANN Fellowship to the first author and a Humboldt Research Award to the second author have supported this research. The authors would like to thank Khai N. Truong, Charlotte P. Lee, Sameer Patil, Yang Wang, Daniel Avrahami, Joe Tullio, Jennifer Rode, Amanda Williams, and Elaine Huang for their comments on earlier versions of this paper.

REFERENCES

1. Beckmann, C., Consolvo, S. and LaMarca, A. Some Assembly Required: Supporting End-User Sensor Installation in Domestic Ubiquitous Computing Environments. *UbiComp 2004: Ubiquitous Computing*, Nottingham, England, 2004, 107-124.
2. Beckwith, R. Designing for Ubiquity: The Perception of Privacy *IEEE Pervasive Computing* 2(2), 2003, 40-46.
3. Boslau, M. and Lietke, B. C. RFID is in the Eye of the Consumer - Survey Results and Implications. *Marketing from the Trenches: Perspectives on the road ahead.* 2006, 1-19.
4. Brotherton, J.A. and Abowd, G.D. Lessons Learned from eClass: Assessing Automated Capture and Access in the Classroom. *ACM Transactions on Computer-Human Interaction 11* (2), 121-155.
5. Brown, B., Taylor, A., Izadi, S., Sellen, A., Kaye, J. and Eardley, R. Locating Family Values: A Field Trial of the Whereabouts Clock. *UbiComp 2007: Ubiquitous Computing*, Seoul, South Korea, 2007, 354-371.
6. Capgemini. RFID and Consumers: Understanding Their Mindset, 2004.
7. Consolvo, S., Rode, J.A., McDonald, D. and Riley, C. Developing Privacy Personas: Handling Inconsistencies in Attitudes & Behaviors, Intel Research Seattle Tech Report, 2005.
8. Hayes, G.R., Kientz, J.A., Truong, K.N., White, D.R., Abowd, G.D. and Pering, T. Designing Capture Applications to Support the Education of Children with Autism. *UbiComp 2004: Ubiquitous Computing*, Nottingham, England, 2004, 161-178.
9. Hayes, G.R., Poole, E.S., Iachello, G., Patel, S.N., Grimes, A., Abowd, G.D. and Truong, K.N. Physical, Social, and Experiential Knowledge in Pervasive Computing Environments. *IEEE Pervasive Computing*, 2007, 56-63.
10. Honess, T. & Charman, E. Closed Circuit Television in Public Places. Police Research Group Crime Prevention Series Paper 35, HMSO, 1992.
11. Iachello, G. Privacy and Proportionality. College of Computing, Georgia Institute of Technology, 2006.
12. I-Newswire. Grocery Store Loyalty Card Use is Strong Despite Privacy Concerns, 2004.
13. Jensen, C., Potts, C. and Jensen, C. Privacy Practices of Internet Users: Self-reports Versus Observed Behavior. *International Journal of Human-Computer Studies*, 63 (1-2). 203-227.
14. Karas, S. Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance. *Journal of Technology Law and Policy*, *7* (1).
15. Levine, M. SIDE and Closed Circuit Television (CCTV): Exploring Surveillance in Public Space. Chapter in T. Postmes, R. Spears, M. Lea & S. Reicher (eds): SIDE Issues Centre-Stage: Recent Developments in Studies of Deindividuation in Groups. Royal Netherlands Academy of Arts and Sciences: Amsterdam, 2000.

16. Lyon, D. *Surveillance Society: Monitoring everyday life*. Open University Press, 2001.

17. McCarthy, J.F. and Anagnost, T.D. MusicFX: An Arbiter of Group Preferences for Computer Supported Collaborative Workouts. *ACM Conference on Computer-Supported Cooperative Work*, Seattle, WA, 1998, 363-372.

18. Mynatt, E.D., Rowan, J., Craighill, S. and Jacobs, A. Digital Family Portraits: Supporting Peace of Mind for Extended Family Members. *SIGCHI Conference on Human Factors in Computing Systems*, Seattle, WA, 2001, 333-340.

19. Palen, L. and Dourish, P. Unpacking "Privacy" for a Networked World. *SIGCHI Conference on Human Factors in Computing Systems*, Fort Lauderdale, FL, 2003, 129-136.

20. Patterson, D.J., Liao, L., Gajos, K., Collier, M., Livic, N., Olson, K., Wang, S., Fox, D. and Kautz, H. Opportunity Knocks: A System to Provide Cognitive Assistance with Transportation Services. *UbiComp 2004: Ubiquitous Computing*, Nottingham, England, 2004, 433-450.

21. Schilit, B., Adams, N. and Want, R., Context-Aware Computing Applications. *IEEE Workshop on Mobile Computing Systems and Applications*, Santa Cruz, CA, 1994, 85-90.

22. Smith, H.J., Milberg, S.J. and Burke, S.J. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20* (2). 167-196.

23. Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, 2004.

24. Solove, D.J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 2007, 44.

25. Spiekermann, S. Privacy Enhancing Technologies for RFID in Retail- An Empirical Investigation. *UbiComp 2007: Ubiquitous Computing*, Innsbruck, Austria, 2007, 56-72.

26. Truong, K., Abowd, G. and Brotherton, J. Who, What, When, Where, How: Design Issues of Capture & Access Applications *Ubicomp 2001: Ubiquitous Computing*, 2001, Atlanta, GA, 209-224.

27. van de Garde-Perik, E., Markopoulos, P., de Ruyter, B., Eggen, B. and Ijsselsteijn, W. Investigating Privacy Attitudes and Behavior in Relation to Personalization. *Social Science Computer Review*, *26* (1). 20-43.

28. Want, R. "RFID: A Key to Automating Everything." Scientific American, Jan. 2004, 56-65.

29. Wild, C.J. and Seber, G.A.F. *Chance Encounters: A First Course in Data Analysis and Inference*. Wiley, 2000.

30. Zureik, E., Harling-Stalker, L., Smith, E., Lyon, D. and Chan, Y. E. *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*. McGill-Queen's University Press, Kingston, ON, Canada, Forthcoming 2008.