Pers Ubiquit Comput (2010) 14:53–72
DOI 10.1007/s00779-009-0229-4

ORIGINAL ARTICLE

Information privacy in institutional and end-user tracking and recording technologies

David H. Nguyen · Gillian R. Hayes

Received: 16 February 2009 / Accepted: 9 March 2009 / Published online: 17 April 2009

Abstract This paper presents an analysis of attitudes towards everyday tracking and recording technologies (e.g., credit cards, store loyalty cards, store video cameras). This work focuses on both *institutional* and *end-user* tracking and recording technologies. In particular, this paper describes (1) an empirical interview and survey study of everyday institutional tracking and recording technologies and (2) an analysis of these empirical data against a framework originally used to describe tension points for end-user tracking and recording technologies. Results from the study demonstrate that people can be highly concerned with *information privacy* while simultaneously reporting significantly less concern regarding the use of everyday technologies that have the capabilities to collect, process, and disseminate personal information. The empirical results and theoretical analysis identify and begin to explain this dissonance. Furthermore, we provide extensions to the analytic framework for capture and access technologies to address differences, similarities, and interplay between institutional and end-user tracking and recording technologies. The results of this paper contribute to the fields of personal and ubiquitous computing by providing significant insight relevant to the evaluation, design, deployment, and adoption of new tracking and recording technologies.

D. H. Nguyen (✉) · G. R. Hayes
Department of Informatics, Donald Bren School of Information and Computer Sciences, University of California, Irvine, USA
e-mail: dhn@ics.uci.edu

G. R. Hayes
e-mail: gillianrh@ics.uci.edu

Keywords Information privacy · Tracking and recording technologies · User attitudes · Institutional · End-user

1 Introduction

Two common research themes in ubiquitous computing are automated capture and access [44] and context-aware computing [1, 38]. Their application spans a variety of domains including education [7, 16], healthcare [3], interpersonal relationships [8, 31], personalization [29], and automation [47]. 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[1] (TRTs) hold the potential to advance these research areas and address a myriad of domain problems, they may also invoke a variety of privacy-related concerns.

Thus, researchers in Ubicomp have long investigated privacy-related issues and concerns surrounding TRTs. These investigations have often uncovered generalized concerns about the recording that is inherent in Ubicomp systems (e.g., [2, 21, 41]). At the same time, however, other investigations have indicated that people are not concerned with many new Ubicomp technologies (e.g., [8, 35]). There is, however, a distinction amongst the TRTs, which have been thus far treated as one group of Ubicomp

[1] Though combined into one group in this paper, tracking and recording technologies are not interchangeable. Not every tracking technologies record (e.g., GPS) and not every recording technologies track (e.g., voice recordings).

applications. The distinction is between *institutional* and *end-user* TRTs. We use the term institution here somewhat broadly, invoking Berger and Luckmann's notion that institutions are any "reciprocal typification of habitulized actions by actors" [5, p. 54]. Institutions inherently modulate the options available to individual action, and thus, TRTs controlled by these entities need to be examined in a different light than those controlled by individual end-users. End-user TRTs are installed and used by individuals and groups of end-users. For example, the Personal Audio Loop (PAL) [17] is a mobile device for augmenting human memory through a short buffer of recorded audio. As another example, the Whereabouts Clock [8], although framed as an awareness tool, involves the gathering of location data for members of a family. Certainly, end users are operating and making choices on their use of TRTs within the constraints of a myriad of such institutions and their perceived cultural norms. In this analysis, however, we purposefully differentiate the reactions to and understanding of TRTs developed, deployed, and controlled by those "collectivities containing considerable numbers of people" and bringing about social control [5, p. 55] from those TRTs adopted by and used primarily towards the end goals of individuals or small groups whose membership is minimally defined and often dynamic.

This paper expounds on the differences in affordances, features, understanding of and reactions to these two distinct types of TRTs. In Sect. 2, we present the empirical methods that serve as the basis of this analysis. This study focused on eliciting specific concerns regarding specific technologies in the concrete context of everyday retail and financial transactions. During this investigation, we also interrogated more generalized current attitudes towards TRTs. Finally, we examined how attitudes in specific contexts with regard to specific technologies may or may not relate to or depend upon general *information privacy*[2] concerns. In Sect. 3, we describe the results of this empirical investigation. Participants in the study reported high levels of information privacy concerns but much lower levels of concern for TRTs in retail transactions and in other everyday activities. The results presented identify and begin to explain this discrepancy. In Sect. 4, we engage the differences and similarities between end user and institutional TRTs by examining the results of these empirical data against a set of seven tension points developed from previous empirical work surrounding end user TRTs [14, 19]. Using this framework, we further analyze the potential tension points in the design, use, and policies surrounding the studied *institutional* TRTs, noting where the framework breaks down and extending it when necessary to consider the particular concerns of capture technologies implemented and used by larger institutions.

This work identifies and specifically interrogates ways perceptions are constructed around both institutional and end-user TRTs. This distinction enables new understanding about the design and use as well as policies around TRTs. The results of this work contribute to the personal and ubiquitous computing community in understanding and supporting the evaluation, design, deployment, and adoption of both novel and known institutional and end-user TRTs.

2 Method

We used a mixed-methods approach to study how individuals in two areas of the United States experience, perceive, and understand a variety of everyday TRTs. 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; however, they are ubiquitous, mostly well known, and represent a broad sampling of technological capability and contextual use.

In addition to being ubiquitous, these specific technologies were chosen because they are also capable of—and in fact for most of their domain uses require—tracking and recording. For example, people use credit cards for a multitude of reasons. Some use them for the convenience of not having to carry around physical cash money. Some use them to gain greater purchasing power. Whatever the reasons, however, credit card companies record every purchase made using a credit card. In fact, it is those records that in some cases encourage people to use the services (e.g., monitor spending to stay within budgets). Those records include not only the amount of money exchanged in the transaction, but also data such as the date and location of the transaction as well as the names and other information about the parties involved in the transactions. As another example, the second technology in focus in this work, store loyalty cards, is marketed as mechanisms for shoppers to receive discounts. When used, they record data such as when the purchase was made, where the purchase was made, and every item purchased during that transaction. Likewise, electronic toll collection systems are often perceived to save their users time and money, because they offer a discount and expedited passage through the toll. When used, they record the time and location of the devices that pass the tollbooths. Unlike these more specific technologies, we also probed understanding of and attitudes towards web servers, which

[2] Information privacy refers to "the ability of the individual to personally control information about one's self" [39].

provide a seemingly endless array of information. Web servers record every visit made to them, including the IP address of the visitor, a timestamp of the visit, the previous page, and the page requested. Likewise, although situated in a narrowly constrained place, store video cameras capture a wide variety of rich information, including the activities of shoppers in their field of view, that can be processed to track individual shoppers as they come into the store and walk about. Despite the enormous amount of data recorded by these cameras, they are often viewed as necessary security measures for the sake of the store or in some cases the customers. Finally, we probed respondents about consumer level RFID, such as that in use on everyday items for inventory control. This technology and its use were relatively novel to participants, with only a small minority declaring themselves familiar with it. In these cases, participant experiences with RFID were restricted to keycards for accessing secured buildings or rooms and tags in consumer goods. It is not yet clear what can or will be tracked about individuals using RFID. If tags are not removed or deactivated from consumer goods, they could be tracked even at some distance for years after a purchase. Likewise, the use of tags to open secured areas can have the added effect of logging an individual's movements in new ways that traditional manual keys could not. These technologies, when considered together, provide a diverse set of tracking and recording experiences from which to situate participant responses.

Our approach included the use of a questionnaire to gauge participant attitudes quantitatively, and a follow-up interview focused on their rationales for those attitudes. We recruited participants from 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. Using that framing as a basis for a more generalized discussion, we also queried people about a variety of everyday TRTs and the privacy—related considerations they engender. That is to say, participants were provided study descriptions that focused on RFID but questionnaires that covered a variety of topics. 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.

2.1 Participants

Fifty-four participants (27 females, 27 males) were recruited at seven sites during the months of May 2007 through August of 2007. Recruitment was done at a variety of shopping malls in two primary geographic areas:

(A) a high-end[3] outdoor mall, a midrange[4] 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 ($n = 36$).

These two geographic areas were picked based on their reported census differences.[5] Southern California is more developed and urban; Southern Louisiana is less developed and more rural. See Table 1 for demographic differences between the two sites.

Table 1 Geographical differences

	Southern California	Southern Louisiana
Median income (2004) (US: $44,334)	$58,605	$37,726
Percentage with Bachelors' degree or higher (2006)	30.8%	12.3%
Percentage of high school graduates (2006)	79.5%	67.1%
Caucasian population	78.8%	73.6%
African-American population	1.9%	18.8%
Asian population	16.1%	1%
Median value of owner-occupied housing unit (2000) (US: $119,600)	$270,000	$80,500

Participants represented a wide range of demographic profiles. They were nearly evenly divided into three age groups: 18–29, 30–50, 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 (see Table 2 for details of participant demographics).

[3] High-end malls contain boutiques and stores that cater to designer brands. These malls have full-service restaurants.

[4] Midrange malls are 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.

[5] http://quickfacts.census.gov/qfd/states/06/06059.html and http://quickfacts.census.gov/qfd/states/22/22109.html

Table 2 Demographic of study population

Demographic characteristics $n = 54$		Respondents % (#)
Gender	Male	50 (27)
	Female	50 (27)
Age	18–29	31 (17)
	30–39	19 (10)
	40–49	20 (11)
	50–59	19 (10)
	Over 60	11 (6)
Race	Asian	7 (4)
	African-American	9 (5)
	Caucasian	80 (43)
Location	CA	33 (18)
	LA	67 (36)
Marital Status	Single	33 (18)
	Married/domestic partnership	58 (31)
	Separated	2 (1)
	Divorced	7 (4)
	Widowed	0 (0)
Education level	Less than HS	2 (1)
	High school grad	22 (12)
	Some college	37 (20)
	College grad	15 (8)
	Some graduate school	7 (4)
	Graduate or Prof. school grad	17 (9)
Income level ($n = 52$)	Less than $30K	40 (21)
	$30K - $60K	33 (17)
	$60K – $100K	13.5 (7)
	Over $100K	13.5 (7)

2.2 Recruitment

We recruited participants in public sitting areas and "food courts" at each site. Systematically approaching everyone in the chosen area, we invited every adult (at lease 18 years of age) to participate in the research study. When every potential participant in the sitting area or food court had been approached, we 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 3–4 h.

In addition to direct recruitment at these sites ($n = 36$), an additional 18 participants were recruited through snowball sampling—asking participants to advertize the study to others in their social circles who might be interested in participating. 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 TRTs are currently used, participants were encouraged to complete the study at the mall. Participants each received a $10 gift card as compensation for time spent during the interviews.

2.3 Procedure

When a person agreed to participate, we first asked the participant about any prior knowledge of RFID or its applications. Prior knowledge was documented (13% had prior knowledge), but regardless of any prior knowledge every participant was then shown the same diagram of the usage of RFID [47], 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 the participants' questions had been answered, they completed a pen and paper questionnaire of 116 questions (described in the following section). We 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 min per participant.

2.4 Survey apparatus

The survey included four primary sections, with each section focusing on a different subject:

- RFID
- Information privacy
- Other everyday TRTs
- Demographic data.

The section dedicated to RFID included Boslau's questionnaire design [6]. 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, corporations, and/or the government. The potential benefits presented to participants included warranties without receipts, returns without receipts, verification of authenticity of products, faster checkouts, automatic microwave cooking instructions, automatic washing machine instructions, recommendations, and getting information about product recalls quickly.

Section 2 contains the Smith et al. [39] privacy instrument. This instrument is a parsimonious questionnaire consisting of 15 questions. This section was included to allow for a comparison of the participants in this study with those in Smith et al. regarding their attitudes towards information privacy. This instrument divides information privacy into four subscales of concern: 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. The *Errors* subscale 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.

Section 3 includes questions about a series of everyday TRTs 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. Questions included the number of years the participant had used a particular technology and how concerned the participant was that records were kept when the technologies were used.

Section 4 includes 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 [43].

2.5 Analysis

We took multiple passes through the data using grounded theory techniques to build a model for how participants encounter and understand everyday TRTs [42]. This approach enabled the use of the qualitative empirical data we had collected to begin explaining and more deeply understanding trends observed in the quantitative questionnaire responses.

We also conducted a comparative quantitative data analysis, but were somewhat 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. Specifically, the Smith et al. instrument combines 15 Likert-scale questions into four subscales, which were the values reported. For discrete data, t tests can be inappropriate and report a significant difference when significance would be more difficult to report using a non-parametric test. To verify the significance of differences between the Smith et al. population and this study's population, a comparison of the discrete data would be necessary.

Within the results collected here, we used standard statistical measures to identify trends of interest, which are reported in Sect. 8 of this paper. T tests were used if the variables were normally distributed. For non-normal data, non-parametric tests were used. For example, for correlations, Pearson's r was calculated for normally distributed data, while Spearman's rho was calculated for ranked data. The results of these comparisons are described more completely in Sect. 8.

3 Results

In this work, we focused on six ubiquitous 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 of these technologies for multiple years. Most participants declared themselves to be familiar with electronic toll-collecting systems ($n = 43$, 80%), but very few had installed them in their cars ($n = 10$, 19%). Fewer participants described themselves as familiar with RFID ($n = 7$, 13%). These numbers confirm that RFID is a *novel* technology. The other five technologies (including electronic toll collection) can be categorized as *everyday* technologies. This distinction becomes important in understanding the results of this work, because experiences with everyday technologies are so impactful on both how people construct meaning around those technologies but also in how they model and understand new technologies when they first encounter them or when they first begin to learn of them.

The remaining sub-sections include quantitative results indicating participants' levels of concern towards information privacy and towards everyday TRTs. Thereafter, we present results from interviews that explain some of the observations from the numerical data.

3.1 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. [39], using the same privacy instrument as those authors (see Table 3). As noted in the

Table 3 Comparison of Levels of Concern on a 7-point Likert scale (higher values indicate higher concern) between the average level of concern reported by the participants of in this study and the average of the Smith et al. studies [39] reported in 1996

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

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

analysis section, the differences presented in Table 2 are only *potentially* significant. For a more conclusive comparison and analysis with the Smith et al. population, the original data from those studies are required. Unfortunately, Smith et al. only reported the means, standard deviations, numbers of participants, and very little information regarding demographic data. There are a multitude of potential explanations for the differences observed, none of which can be guaranteed to be accurate. Some issues, do, however, stand out and so are worth noting here. First, the differences in the 'unauthorized secondary use' and the 'improper access' subscales (and consequently the 'overall' scale) may be attributable to time. Smith et al.'s study #1 was done in Fall of 1992. Studies #2 and #3 were done in Spring of 1993. Data for this study were collected in Spring and Summer of 2007. There is a span for almost 15 years between the studies. In that time, the world has experienced massive increases in e-commerce, email, and use of the Internet in general. These increases have also brought a greater awareness of threats such as identity theft and phishing. Interestingly, many have argued that over time so-called privacy concerns will diminish as we habituate to a world in which we are watched and tracked [11, 25, 27, 30]. These data, however, potentially tell a different story, one in which increased exposure may actually be increasing the concerns people report for general information privacy.

Furthermore, the demographics of the participants in the various studies differ. Smith et al.'s first study sampled a group of graduate business students from an east coast American university. Their second study sampled undergraduates from an east coast American university. Their third study sampled American members of an international IT governance professional association. Gender and age distributions of the three studies are not reported. In our study, however, the intent of this study was to sample shoppers in general, thus only a small subset of the participants were students or professionals similar to Smith et al.'s population.

Within the demographics of our subject population, most groups responded similarly to one another on the information privacy subscales. 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.

3.2 Attitudes towards everyday tracking and recording technologies

Participants rated their levels of concern with the five studied everyday TRTs: store loyalty cards, credit cards, security cameras, electronic toll collection, and web servers. Ratings were given regarding concerns about each technology on a seven-point Likert scale ranging from "strongly agree" (7) to "strongly disagree" (1) (see Table 4 for the specific wording and numerical results of these ratings). With the exception of web server records ($\mu = 4.43$, $\sigma = 1.90$), participants reported low levels of concern 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 Fig. 1). Furthermore, the responses indicate a discrepancy between the stated generalized information privacy concerns and the stated concerns for some everyday TRTs.

The levels of concerns of the everyday TRTs are not only different when compared to the level of concern for information privacy, they are also different among themselves [Pearson $\chi^2(24) = 46.7399$, $p = 0.004$). Unsurprisingly, this result suggests that concern levels change depending on the type of technology queried. More interestingly, responses to all of the everyday TRTs are correlated positively with responses to at least one other technology (see Fig. 2). Store loyalty cards, web servers, and credit cards have a strong correlation ($0.6 < r$ or $\rho < 0.8$) to each other, suggesting that participants tend to treat these three technologies similarly. Cameras have a moderate correlation ($0.4 < r$ or $\rho < 0.6$) to store loyalty cards and credit cards. Electronic toll collection is moderately correlated ($0.4 < r$ or $\rho < 0.6$) to store loyalty cards and web servers. Last, not only are the levels of concern for information privacy different from the levels of concern for everyday TRTs, they are also not significantly correlated to any of the studied everyday TRTs. These correlations suggest avenues for future research in exploring how these technologies, and people's understandings of them might be related to one another.

Table 4 Concern for everyday technologies on a 7-point Likert scale (higher values indicate higher concern)

Technology	μ (σ) (n)
Credit card	3.65 (1.71)
"I am concerned that my credit card purchases are recorded."	$n = 52$
Store loyalty cards	3.47 (1.71)
"I am concerned that my purchases at stores can be tracked when I use their loyalty card."	$n = 49$
Electronic toll collection	1.93 (1.68)
"I am concerned that the electronic toll collection system has a record of my trips on the toll roads."	$n = 43$
Web server records	4.43 (1.90)
"I am concerned that websites have a record of my activities when I visit them."	$n = 53$
Store video cameras	2.85 (1.87)
"I am concerned about the surveillance cameras in stores."	$n = 54$

3.3 Attitudes towards RFID

In addition to assessing how people have come to understand and use everyday TRTs in relation to their generalized understandings of and concerns about information privacy, one of the goals of this work was to interrogate a common but

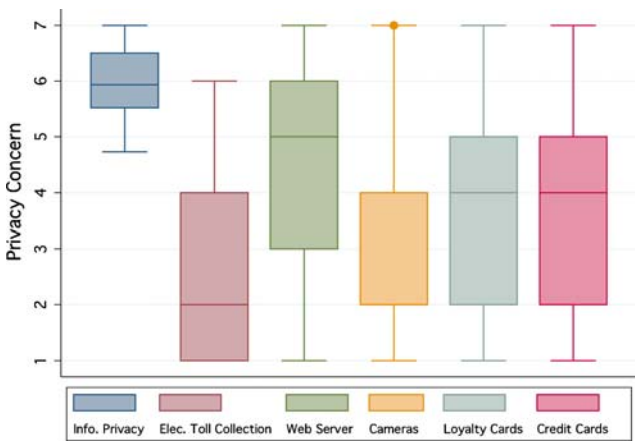

Fig. 1 Information Privacy Concerns versus Everyday Tracking Technologies Concerns *box plot* (higher values indicate higher concern). In this figure, the much higher concern for information privacy over any of the specific everyday TRTs can be easily seen

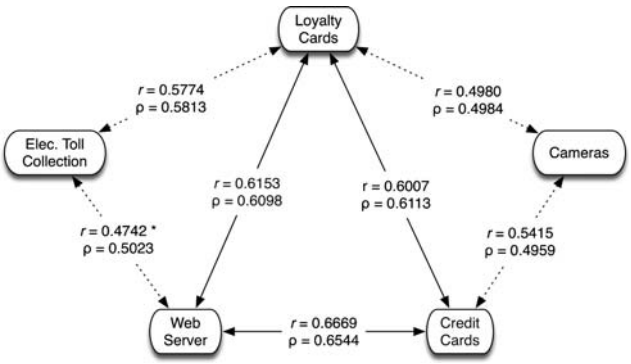

Fig. 2 Correlations of Everyday TRTs $*p < 0.002$, all other $p < 0.001$. *Dotted lines* indicate a moderate positive correlation; *solid lines* indicate a strong positive correlation. For completeness, both Pearson's r and Spearman's rho are calculated and presented

relatively unknown ubicomp technology. In this case, we chose RFID to serve as that technology. The results of this work indicate that RFID is relatively unknown within this subject group. Of the 54 participants, only seven 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 [41], but is low in comparison with the 23% of US participants who reported being knowledgeable with RFID in a Capgemini study [9] or the 38% of US participants in the Queen's University international survey on surveillance and privacy [49].

The majority of participants responded that the potential benefits of RFID outweigh its 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 survey also included questions about concerns about tracking through RFID by four different entities: strangers, the government, thieves, and companies. For each entity, participants also responded to 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 to produce a level of concern for each entity (see Table 5; Fig. 3). Furthermore, these results indicate that the stated information privacy concerns and the stated concerns for tracking by RFID are more similar than the stated concerns of everyday tracking technologies.

Despite the high levels of concern observed for RFID tracking by stranger, government, thieves, and companies, those levels are still significantly different from the levels of concern reported for information privacy (see Table 5).

Table 5 Concern for RFID tracking on a 7-point Likert scale (higher values indicate higher concern)

RFID Tracking by	μ (σ)	Compare to 'overall' Information Privacy 6.00 (0.59)
Strangers	5.18 (1.43)	$p = 0.0000$
		$t = 4.4591$
		$df = 53$
Government	4.91 (1.79)	$p = 0.0000$
		$t = 4.7860$
		$df = 53$
Thieves	5.45 (1.55)	$p = 0.0086$
		$t = 2.7292$
		$df = 53$
Companies	4.50 (1.67)	$p = 0.0000$
		$t = 4.9985$
		$df = 35$

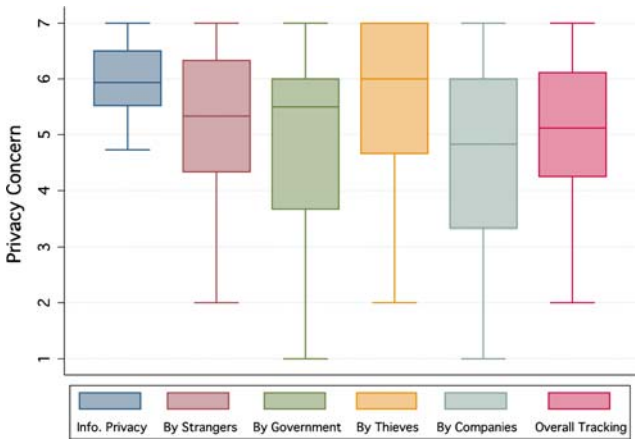

Fig. 3 Information Privacy Concerns versus RFID Tracking Concerns *box plot* (higher values indicate higher concern). In this figure, the concerns for RFID tracking are high and more aligned with the concern for information privacy

A one-way ANOVA shows that there are differences among the four entities ($F(3, 194) = 2.74$, $p \leq 0.05$). This result suggests that the reported levels of concern are dependent on the entity doing the tracking. Moreover, the entities are correlated to each other (see Fig. 4). Reported concern for tracking by thieves is moderately correlated to reported concern for tracking by government ($r = 0.4151$, $p < 0.01$). All other pair-wise comparisons are strongly positively correlated ($r > 0.6$, $p < 0.0001$). These correlations suggest that the levels of concern participants have about RFID tracking are somewhat stable regardless of who is doing the tracking. Reported concern for information privacy is weakly positively correlated to RFID tracking by strangers, government, and thieves (all $r < 0.4$)

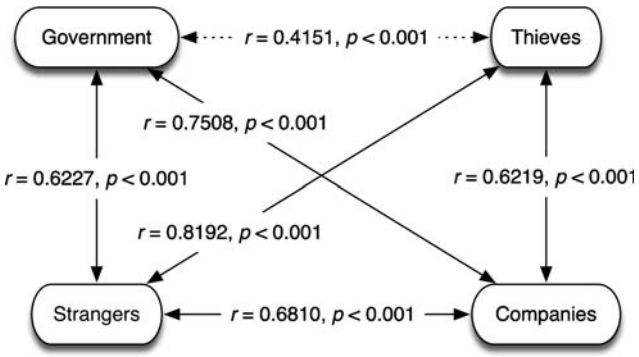

Fig. 4 Correlations of Tracking Entities *dotted lines* indicate a moderate positive correlation; *solid lines* indicate a strong positive correlation. There is a correlation among the entities, but the levels of concern are not the same

and not significantly correlated to tracking by companies. Finally, when asked to weigh the potential advantages and the potential disadvantages of RFID, the majority of participants reported favoring the potential advantages. This response is not correlated with concern for information privacy ($p = 0.2707$), but is moderately negatively correlated to overall RFID tracking ($r = -0.4993$, $p < 0.001$). This result suggests that even though participants are concerned about the notion of being tracked, they still favor the potential advantages over the potential disadvantages, such as the ones described in the questionnaire.

3.4 Comfort with recording and tracking technologies

During the analysis of the qualitative empirical data collected during this study, three overarching themes surrounding comfort with everyday TRTs were identified:

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

This section details each of these themes and present empirical evidence demonstrating their impact on the attitudes of interview participants.

3.4.1 Threat comprehension

Participants reported a clear understanding of potential benefits of recording and tracking technologies. For example, they nearly all commented on the ease of use of credit cards for shopping. They were approached during in a shopping area and so may have been more readily predisposed to be considering credit cards in depth. However, at the same time, they struggled to articulate possible costs or threats of these very same technologies. For example, participants often struggled to describe any problems with credit card records. Only after being pressed repeatedly in most cases would they 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 [24]. 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 mostly irrelevant or harmless. For example, when asked about the records produced through store loyalty cards, one participant acknowledged an abstract potential threat, but commented how they are relatively harmless:

> 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 a purchase was made in the event that the shopper needed to return it or apply for a warranty. Several participants described uses of electronic toll collection records as alibis or otherwise relating them to legal actions that would require evidence of a person's location. Recording and tracking of everyday activities were often reported to be irrelevant or harmless as compared to other potential threats, such as thieves. For example, 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."

Although some participants intoned that they should be concerned, others avoided thinking about the threats, despite acknowledging fear of the situation. For example, for one participant the best coping strategy for dealing with ambiguity about the use of information in store loyalty cards, was simply to ignore 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 inaccurate mental models of the inner workings of technologies, which may have further contributed to challenges in understanding the potential threats of these technologies. This phenomenon is aligned with the findings of Patil and Kobsa, in which participants with an inaccurate mental model of the underlying technology of instant messaging were less concerned about privacy issues [34]. In our work, however, an opposite phenomenon was primarily observed. Those participants with inaccurate models of the workings of the technology tended to assume a more dangerous position than is correct, perhaps explaining why RFID was rated to be of more concern than electronic toll collection, which is a specific and known RFID technology. 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, web server logs do not contain passwords or other account information. Despite this technological impossibility, concerns about web tracking technologies were significantly more common than the other everyday TRTs queried, such as pervasive video surveillance, which participants tended to understand more accurately.

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 [40], it represents an important challenge in the discourse and design surrounding TRTs as well as in 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 [33].

3.4.2 *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 TRTs. This result echoes some of the results of other researchers more specifically focused on CCTV [20, 26, 28]. This attitude was compounded when the TRTs were included as part of a service. For example, the records created as part of the electronic toll collection—both those from the RFID scans and the photographs of each license plate as drivers proceed through the gates—were seen as an inherent part of service use. Many participants commented that the recording was a small price one had to pay to get the services.

Participants also largely seemed to hold 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. Although some participants reported trusting corporate information use to be regulated by the government, corporations were often seen as having the highest potential to abuse the information they were collecting. Some behaviors imagines by the consumers we interviewed were considered abuses even though technically legal. For example, 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… it's a profit business.

When asked about the same issue, another participant, with a less negative attitude towards corporations, was not as concerned. As we will describe in the next section, attitudes (particularly trust) towards the tracking and recording entity affect an individual's attitudes towards the technology itself. For this participant, he is 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 [49]. 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 is that individuals would be hidden in the large databases. This deindividuation in a crowd 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.

3.4.3 Situational dynamics

General beliefs may not always coincide with beliefs in specific situations (see Figs. 1, 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 tracking and recording in shopping contexts. As shown before in different domains, users' stated beliefs do not always coincide with their actions (e.g., [23, 45]). Although we 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 [39] queries participants about information privacy in general. However, when asked about specific TRTs, 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 higher 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 […] 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. Therefore, without other available options, people may be "forced" to use a particular technology or service nullifying any other risk or cost analysis done in relation to the benefits or necessities.

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, depending on the particulars of a situation (e.g., options that are perceived to be available), concerns may be raised or lowered.

3.5 Discussion of results

Explanations for the discrepancy between participants' attitudes towards everyday TRTs and their fears and concerns are grounded in the data and reveal the three factors described in detail in this section. First, many people may not understand the collection, processing, and dissemination of recorded consumer data (threat comprehension). Second, they may not carry a "reasonable expectation of privacy" to use the legal terms (expectation of privacy). And last, some situations are likely to provoke more concern and action than others (situational dynamics). These three major factors are laden with other issues, some of which are influenced by more than one of these factors at once, however, and are worthy of more discussion:

- General notions of privacy versus specific technologies,
- Novel versus everyday technologies, and
- tracking and recording that is done by end-users versus those done by institutions.

The ability to gather reliable, grounded, and accurate responses from individuals about privacy and related concerns in information technology continues to be a struggle within the Ubicomp community. The nature of the questions in the study or the nature of the technologies studied themselves will likely always be factors in identifying potential concerns, whether designing or evaluating ubicomp technologies. In this study, we asked participants

about general concerns for information privacy. However, in the same study, we also asked them about specific technologies. The specific technologies queried were not reported to be bad or unwanted technologies. The participants, in fact, favored many of the technologies and the services they provide, not unlike other ubicomp technologies that are studied in quasi-controlled deployments and are providing a positive experience for the participants (e.g., the Whereabouts Clock [8], eClass [7], and Tivoli [36]). Thus, when asked if these "positive" technologies are of any concern, participants may be less willing to say so. Contrast these studies with those in which participants had less positive or even negative experiences with the services provided, and there may be an effect on the level to which the non-functional concerns and requirements became of greater importance (e.g., Active Badge [46] or Virtual Kitchen [22]).

The challenges between reactions to specific technologies and generalizable questions and concepts are likely impacted by all three of the factors described in detail in previous sections. When discussing general concerns, it may be difficult for people to imagine and comprehend much less verbalize the specific threats engendered by a wide range of technologies. On the other hand, when dealing with specific technologies, these threats may be more comprehensible but not generalizable, thereby skewing the results. Likewise, expectations of privacy may be extremely specific based on technology used and the legal and culture norms of their environments. For example, audio recording is tightly legally regulated, whereas photography may be less so in many states. This example leads directly into the issue of situational dynamics. Clearly, discussions about general concerns are unlikely to consider situational dynamics unless participants spontaneously offer detailed examples or the researchers are careful to include such questions and probe them directly. Even when discussing specific technologies, however, few are limited to a small set of likely situations and still require careful planning of the research questions to include issues of situational dynamics. Overall, the challenge of asking appropriate research questions to get at the needed level of specificity, familiarity, and so on is likely to continue to be a challenge for the ubicomp community as more and more technologies that inherently include tracking and recording become part of research and commercial agendas, warranting substantial further investigation.

As ubicomp technologies become more and more engrained in everyday experiences—in the form of mobile phones, mobile music players, ultra-large screens embedded in the physical environments, GPS units in cars and phones, and more—the Ubicomp research community is left with the challenge of understanding concerns related to information privacy, the control of data, and so on with both novel research technologies and those that have been adopted *en masse*. Novel technologies may not have existed long enough for people to understand and be aware of possible risks and threat models—the so-called "novelty effect" of research deployments. However, length of experience does not necessarily add to understanding and awareness of risks and threats of a technology. The potential for differences between novel and familiar technologies is important to consider moving forward and again crosses multiple factors described in the previous sections.

In this study, we queried individuals about both everyday familiar technologies and a relatively novel one. In his analysis of tracking and recording technologies for eldercare, Beckwith reported that the participants in that study did not understand the technology [3]. Beckwith showed that people are not capable of understanding the privacy tradeoffs of novel technologies. This study echoes his points and demonstrates that people do not comprehend the tracking and recording capabilities of novel technologies like RFID, and furthermore not of everyday technologies either. Therefore they are likely not capable of understanding the privacy tradeoffs of everyday technologies either. In contrast to the short-term interaction with novel technology in the Beckwith study, participants of this study have used the everyday TRTs regularly for multiple years. Even then, they struggled to identify and verbalize risks and threats incurred from these technologies. Use of these technologies on a daily basis without incident likely influences perception of risk. The current lack of incidents may also impact expectations of privacy. Tracking and recording is often seen as an integral part of familiar technologies. Having regularly interacted with the records themselves (e.g., credit card statements), people understood recording to be an unavoidable if not beneficial part of the service they were using. They do not have the technical knowledge to conceive the service without the use of TRTs. This belief of being unable to separate the service from the tracking and recording often carried over in participant discussions about novel recording technologies as well. Thus, the situational dynamics may not depend so much on the "novelty effect" as they may depend more on one technology being different from the next, novel or otherwise.

Finally, the entity doing the tracking and recording—whether an end-user, group of end-users, or a major institution—may also be a factor in the rationale for assessing concern. In this work, we focused on institutional TRTs. The focus of much of the Ubicomp community on capture and access applications [1, 44], which are in large part dependant upon end-user TRTs, lends itself to analysis of the differences between these types of TRTs. Again, these

issues are observed across all three factors described in the previous section. By classifying the TRTs in this study according to what institutions and people might control them and have access to the records they create, people were able to incorporate their feelings about those institutions and individuals into their comprehension of threats. Expectations of privacy are not static [4, 33] and may be substantially influenced by differences in experiences with individuals as opposed to institutions as well as the specific situations being considered at the time. This final issue of examining differences between institutional and end-user TRTs is an area for substantial future research. In the following section, we explore this issue further by analyzing the data from this study about institutional TRTs against a framework initially designed for end-user TRTs.

4 Comparing end-user and institutional tracking and recording technologies

We previously proposed a framework through which one can attempt to design adoptable capture technologies and against which one can evaluate their impacts that included seven tension points: ownership of data; choice; visibility and awareness of recording, archival, and deletion; trust; features of rich media; face; and decision point [14]. This framework, like much of the research in capture and access applications, was only applied to what we call end-user TRTs. In this section, we use this framework to examine the studied institutional TRTs, noting where the framework breaks down and extending it to consider the particular concerns of TRTs implemented and used by larger institutions.

4.1 Ownership of data

Knowing who owns and controls the data can allow people to use other methods of negotiation outside of the technology itself to influence when and if recording takes place, the use of data, and so on (e.g., talking to the owner about what is saved and requesting the stopping of recording). In the case of institutional TRTs, the owner of everyday TRTs and data are often large institutions, such as the government or a corporation.

Negotiating with these types of institutions can often be limited or challenging for a variety of reasons. First, these entities may be laden with bureaucracy making it difficult to even find the correct person with whom to discuss any concerns. Second, the available resources of a large entity compared to those of an individual are inherently imbalanced, passing the imbalance on to the negotiation possibilities. In end-user capture and access applications, some of these phenomena can also be present. For example, the owner—even if another individual—may have more power than those who may be subjected to the recording (e.g., teacher's aides being recorded in classrooms at the whim of the teachers [15]), but this phenomenon can be exacerbated when considering large institutions. Finally, common physical indicators of ownership and use, such as where the data are stored, can be hidden in these cases with data storage amounting to trade or government secrets in many cases.

Additionally, even if end-users can identify who initially owns their data and negotiate with those entities, the data can be collected by one corporation and sold or shared with another. Many people, in fact, reported that this kind of sharing was assumed:

> "If you give it to one, the rest of them can get it."

In the results of this work, people most often brought up this concern when considering things that might inconvenience them. For example, people reported being worried that a corporation who bought such data would eventually send spam or junk mail or in some way profit from these data.

> "Because I think what I decide to do, what I decide to buy is my business and anyone who wants that information is only using it for their benefit and they're using my lifestyle as a means to make more money for them and I'm not being compensated for that, nor am I being asked for my permission to do it."

If, on the other hand, the company retained sole ownership of the data, the threat was often perceived as much lower. For example, one person noted:

> "As long as they don't share it with anybody, with no other companies, I don't think it's impacting me negatively."

It should be noted that while personal data and records such as the ones mentioned above may be shared amongst corporations in the United States, the situation is very different in the European Union. The EU Directive 95/46/EC protects individuals with regard to the processing of personal data. Sharing of such data without prior consent would be unlawful in the EU.

4.2 Choice

Choice includes being able to opt in or out of a capture-enabled system or service. The choice may be between using one service over another. For end-user TRTs, some end-users have the choice to initiate or block recording. At the same time, other end-users may have little or no choice. For example, it is often common practice for college

students to audio record class lectures. In this situation, the student doing the recording has control over her recorder. However, her fellow students have little say in whether their questions in the class may or may not be recorded. This disparity in the ability of some stakeholders to make choices about recording while others cannot is even more extreme when one considers institutionally controlled recording. For institutional TRTs, it is the institution that made the choice to initiate the recording. For example, it is the choice of corporations and storeowners to install and record from the security cameras. Thus for the non-controlling end-user, the choices they have are dependent on the relationship they have to the controlling entity. For end-user TRTs, end-users without the technology can negotiate to participate or not. For institutional TRTs, the effective choice is to use the service provided or to avoid the service.

The choice to be recorded may be made by a consumer as simply a "price to pay" for making some other choice—such as using a service.

> "If I don't give them the information, they might not give the product or service I'm looking for. It doesn't matter what I think. If I want a service, I have to comply with their wishes."

These sentiments were echoed in survey and interview responses describing technologies already in use. Additionally, when queried specifically about RFID, the least well known of the technologies studied, one participant responded that the advantages of the technology came with a cost. The following is a comment on RFID's potential for quicker checkout in the shopping experience:

> "You know, if you want to be… to get in and out quick, then you pay the price no matter what. I mean, that's just like anything. You know, you have to pay for what you want for convenience if that's what you want."

Although many choices specifically about recording then are *de facto* made based on choices made for other reasons, the ability to choose at some level can still impact perceptions of these TRTs. For example, in reference to Electronic Toll Collection technologies, one participant commented that:

> "…I still don't have a problem with it because that's a personal choice. That's a choice I make to let you know—you, the collector—know that I'm crossing this bridge at a certain time every day."

Likewise, when considering tracking that may occur online, one person noted, "I use the Internet, being aware of it, that they have that record." Talking about store loyalty cards, another participant said:

> "And in a way you look at it, if it was loyalty card, you signing up for it to be a member of it, to be a part of it. So, in one way you're allowing, like, you're agreeing to them that—to be tracked… It becomes, like, maybe your choice to be monitored for it."

Although many people reported that even if they were not able to make a significant explicit choice, they were at least able to make the choice as part of a tradeoff analysis with other services. In other situations, there may be no alternative but to be recorded. For example, to rent a car in the United States, one needs to have a credit card. One cannot opt out of being recorded by a credit card company when one rents a car. In other cases, people simply do not have the resources or knowledge to avoid these recordings. One participant commented on her need to use store loyalty cards to save money:

> "Yeah, I use that because I'm forced into using it… Ralphs (grocery store) has higher prices, but then if you don't use your loyalty card they charge you a lot of money…"

Aside from situations in which they simply do not have the resources to make a choice about recording, people may actually be able to make such a choice but *perceive* that they have no choice. In those cases, particularly in terms of institutionally controlled recording, people reported being resigned to being tracked because they believed the choice is not ultimately theirs to make. Rather, the institution has already made it for them. As one participant expressed:

> "I'm realistic enough to realize that no matter what my wants and feelings are it's not going to make any difference out there in the market. So I mean, if they do it they do it, if they don't, they don't."

Similarly, people responded that whoever owned the property owned the rights to make a choice about recording it, such as in a private store. Thus, any choices to be made surrounding that recording must be made at a higher level, such as not frequenting that shop:

> "It's their store. I mean, if they choose to have surveillance, it's their store. I don't have to go in there. I can go shop somewhere else."

4.3 Visibility and awareness

Visibility and awareness of recording can have large impacts on how people respond to that recording. Different levels of visibility may inherently be built into the technology or its deployment, sometimes correlating to the information about and awareness of these technologies that

those who might be subjected to recording hold. A significant point for all of the technologies queried in this work is that there is virtually no feedback from the transactions and interactions with these technologies. This lack of feedback sometimes leads to questions of whether the technology is even working (e.g., if the toll collecting device is not functional, you are unlikely to know it until a series of toll violation citations appear in your mailbox one day). This lack of feedback can also have impacts on individual concerns about, acceptance and adoption of, or ignorance regarding everyday tracking and recording in their lives. As one participant puts it:

> "…you're not reminded every time that you do something that somebody's going to be tracking it."

As TRTs weave themselves into the everyday fabrics of our lives, they do indeed become increasingly "invisible in use" [48]. This invisibility manifested itself in our interviews across all of the technologies we queried. Credit cards, so ubiquitous in everyday interactions, were a particularly interesting point because of their seamless use in everyday shopping and financial transactions. For example, one person commented that recording from credit cards is

> "…not something I often think about, but I guess maybe there was a part of me that was kind of aware, but I just—you know, it's just not something you ever really think about."

While visibility and awareness are design issues commonly considered with regard to the moment of interaction, for some participants the effects of the recording could be seen months after the fact, in the form of increased unsolicited mail or traffic citations as in the toll collection example stated previously or in the case of so-called "red light cameras." In the case of increasing "junk mail," the recipient may not even know what caused the increase in solicitations.

The majority of participants expressed wanting increased visibility into the records created about their activities. In particular, with regard to the creation of new technologies, people expressed a desire to make those capabilities and uses more clear in the future. For example, one person, who had resigned himself that new technologies are "going to happen no matter what," still wanted legal oversight of those technologies:

> "They need to pass a law that says 'no eavesdropping on RFID unless you give notice.'"

Despite this push for greater visibility, the results of this work also echo those of past research in that this desire is inherently at a point of tension with another significant user requirement, that of technologies being more "calm" and less intrusive [14, 48].

4.4 Trust

Acceptability of TRTs may depend on the trust of and the relationships among the various stakeholders and technologies involved. That is, trust of an individual for another individual, for a group, for an institution, or for the technology itself all can play a role in the acceptance of TRTs. Trust, in this case, is the individuals' expectation that their information will not be misused or abused.

In this work, we have focused on TRTs, primarily perceived to be controlled by two types of institutions: governmental (federal, state, and local) and business (from small businesses to major corporations). Inherent trust or distrust of those institutions can influence perceptions about recording by these entities. For example, in reference to RFID and the trust she has placed in the corporation controlling it, one participant commented on the mechanism that would further enable that trust:

> "I mean, yes, it might make things a lot faster, and yes, it will probably be better for the store; but the store's best interest should be the customer. I mean, if customers are going to feel, you know, that, like uncomfortable going to the stores they're going to lose service."

When also asked about RFID tracking, another participant was concerned about the tracking done by the government for no reason other than because it was the government. Asked to expound further, the participant explained simply:

> "Because I'm not a fan of the government."

Outside the entities that own or have access of the data, trust in the technology itself impacts acceptance—trust that the technology would work or that the technology was secure. When asked about RFID, one participant was concerned about the security of the technology itself:

> "I guess the only concern I would have about that would be the ability for people to hack into there and be able to get information on someone. But at the same time, because of the way we can track everything I think we're more prepared now to be able to find out who gets in and find them. You know what I'm saying? So, even if you would get hacked, I feel that we could definitely find out who it was…"

4.5 Features of recorded data

The particular types of data, affordances and features of collected data, and capabilities in aggregate form impact the way people perceive the TRTs. The data collected by

the technologies studied in this work include transactional information that can be associated to particular individuals. The data collected are rich in that it contains much information—about individual consumers as well as particular groups of consumers. However, for some participants, there was a perception that there was actually not a lot of information in the type of data that was collected. The data were perceived to be not very useful, whether it was web server records, credit card records, or store loyalty card records. Speaking about web server records and how it can affect one's life, one participant said:

> "I don't think—I can't see it affecting my life any way, shape or form."

One challenge that emerged for technology designers and policy makers is in how little people reported knowing and understanding about the features of the data recorded and the technologies recording them. For example, speaking about store loyalty cards, one participant said:

> "I don't, I mean, I don't know how much information they keep… And I think most wouldn't care if the grocery store knows what kind of groceries you get."

Not knowing the richness of the data collected, another participant said of credit card records:

> "I can't see anybody would want any of that information anyway. Why would that be relevant?"

Although some participants perceived the data collected as neither relevant nor important, others sometimes overestimated the power of everyday TRTs. One participant described how satellites could track individuals no matter where they went:

> "Because anywhere you go you're on satellite so it doesn't really matter. You know you can get satellite views from the Internet at these web sites that you can actually look at your own house?"

In the case where people thought little useful data was collected, they were rightfully not motivated into action. However, on the other extreme, where the perception is that one is recorded via satellite everywhere one goes, people are not motivated into action either, because "it doesn't really matter."

Despite the majority of participants wrongly described at least some piece of technology as being (in)capable of collecting some data, there were others who described concerns based specifically on an accurate understanding of technology's potential. One participant verbalized a legitimate concern of the possibility of collecting such rich data about a person through RFID:

> "They could follow me or track my habits… Here comes more unwanted junk mail… I mean super junk mail."

In this case, acceptance of the technology is not only dependent on understanding the richness and features of recorded data, but also the use of that data. That is, the perceived features and usage of recorded data is another factor in the acceptance of TRTs.

An interesting feature of recorded data that emerged from this study and this analysis that differs from examinations of end-user TRTs is the emphasis on ability to access the same information using different data. That is to say, for some people, being documented or monitored in one way was not a source of concern, because they determined the same could be accomplished in some other way. For example, tracking of individuals does not necessarily have to be done via CCTV because tracking individuals' cell phones could easily get similar data—in fact, probably more easily. Likewise, when describing use of store loyalty cards, one participant noted "they know what I buy anyway; they scan it on the register"

Finally, another interesting finding from examination of these institutional recordings is found in the very masses of data that may be of concern to some. For some, the very richness and quantity of data recorded by these technologies were perceived as a means of shelter. Many participants reported comfort in the inability of large corporations to disambiguate their individual data from the masses. For example, talking about credit card usage, one participant said:

> "There's so many people buying so much stuff on credit cards. How would they target one person or just go look at one person?"

We had posited in a previous study [14] that richer data would be more problematic. That may be the case for end-user TRTs, it does not seem to be the case of institutional TRTs, as shown above.

4.6 Face

A significant challenge to managing one's presentation arises when the "face" presented in one setting can be recorded, removed, and reinserted elsewhere. Face in this case is aligned with Goffman's definition of "an image of self delineated in terms of approved social attributes [13]." People deal with issues of face and manage impression by controlling what is presented about them [12]. In the context of everyday TRTs, without control of what information is collected about them, people will not be able to manage which face is presented under differing situations.

The empirical results of this work indicate that presentation of data out of context was a pressing concern.

4.7 A few people described wanting to know what data about them they are being collected. For example, speaking about how data can be gathered through RFID wirelessly, one participant commented:

> "You don't have any control regarding what information other people can gather from me. It's different. Like, if they approach you [in person], they get this information from you; you know what you're giving out."

One common concern is to have the recorded data taken out of context and used inappropriately later. Though there may be a multitude of reasonable explanations for people's actions, taken out of context, records of their actions can be damaging. As an extreme example, data can be used as potential for black mail as suggested by one participant:

> "Let's just pick a hypothetical example, a married person going in there buying condoms. My wife has had a hysterectomy. Why the hell do I need condoms? You can see the potential implications if that kind of information got into the wrong hands. It's potential for blackmail. Suppose I'm on court ordered program from the court for drunk driving and I'm in there buying alcohol…"

One common separation in the practice of controlling self-presentation and face is the distinction between work and home [37]. People manage a "work face" when they are at work and a "home face" when they are at home. Even in seemingly benign everyday technologies, like Internet use, these concerns of boundaries between home and work emerged in the interviews in this study. For example, commenting on using a computer at work, one participant noted:

> "I make sure I know where I'm at [on-line] when I'm at work that's for sure."

4.8 Decision point

The decision point for when to participate in recording can be done at three major points: before recording starts, during the recording, or after the recording. The decision points are moments in which the available choices can be executed. With end-user TRTs, a person decides when to interact at all three points. With institutional TRTs, the institution decides when to record and what to record. Once deployment starts, the institution retains almost all power over the data.

The only possibility for individuals to execute a choice is to decide whether to use the system or service provided. Individuals are at a decision point every time they interact with or through a service the institution provides. However, as discussed in Sect. 4.2, not all choices given to consumers and end-users are actual choices. The choices made at the decision points depend on more factors than just deciding to opt-in or to opt-out.

With institutional TRTs, the decision points also act as a means of negotiation between the institution and the individual. This negotiation process is thus very limited. There is no way for individuals to directly negotiate with institutions. For example, there is no current way for individuals to set the terms of usage when they agree to use a technology like the electronic toll collection system. If they use the system, they will be tracked. As currently implemented, the system requires the tracking data for billing purposes.

To extend our framework, the institutions face a decision point when they implement a TRT. Continuing with the electronic toll collection example, when it was being implemented, a decision was made (either explicitly or implicitly) to model the system after a credit-card-like system instead of a cash-like system. With a credit-card-based system, records are kept. If it were a cash-based system, different (and perhaps less) records would be kept.

Of course, the same can be said of end-user TRTs. A decision point also exists for that technology during implementation time. The decision at that point is how much tracking and recording is necessary to have the desired functionality.

4.9 Summary of framework application on institutional TRTs

In this section, we explore how institutional TRTs differ from and are similar to end user TRTs. Differences include knowing which entity owns the data collection changes the perception of the people being tracked or recorded. For example, dissemination of collected data to other entities can be perceived as more readily done by an institution than by an end-user. The perception of having a choice is also affected by knowing which entity is doing the tracking and recording. If done by an institution, some people may feel that the institution has already made the choice for them. The point at which a decision is made to participate with a TRT or not is also different between end-user and institutional TRTs. With end-user TRTs, a person can often decide when to interact. With institutional TRTs, the institution may have decided when and what to record. For the institutional TRTs studied, visibility and awareness were seemingly lacking, whereas they are a common trait of end-users TRTs [Bellotti 1993]. And last, trust of the entity

doing the tracking and recording can also be vastly different, simply depending on whether that entry is an individual or an institution. For certain participants, the mere fact that it is the government makes that entity untrustworthy.

Similarities between end-user and institutional TRTs include the rich data collected by all entities. The affordances and features of the data collected by either type of TRTs were often unseen or not understood by individuals being tracked or recorded. Another similarity is the presentation of impression management or face. People were concerned about presenting the appropriate face in both kinds of TRTs. Specifically, they were concerned about data of them being used out of context.

Engaging the TRTs through these tension points reveal to designers and researchers who is doing the recording, who owns the data, who has access to the data, what data is recorded, where is the collection taking place, when is the recording taking place, and why (or for what purpose) is the recording being done. The framework is helpful in designing new TRTs—whether end-user or institutional—and in evaluating current TRTs, but questions about adoptability of TRTs remain.

5 Conclusion and future work

In the last decade, research in Ubicomp has investigated many privacy-related issues and concerns surrounding TRTs. 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 demonstrate 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. [18] described factors that together influence people's decision making about a specific audio and video recording installation. Consolvo et al. and others describe how people might be trading their data and information for the value provided by the product or service [10, 32]. 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.[6]

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

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 TRTs become accepted. In particular, individuals experience challenges to their understanding in two fundamental areas:

1. Their ability to assess potential threats of what is tracked/recorded and how it can be used.
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.

Moreover, the "novelty effect" does not play a strong role in the understanding of risks and threats when it comes to novel versus everyday TRTs. This study shows that participants did not understand the tracking and recording capabilities of everyday TRTs—technologies they have used regularly for multiple years.

The data from this study were also analyzed using a framework designed to evaluate end-user TRTs. There is a difference in assessing ownership of the recorded data when technology is end-user based or institutional based. That class of ownership defines the potential threats resulting from the possible use of the collected data. Moreover, the category of TRTs also defines the options and negotiations possible for an individual with respect to that technology. Thus understanding of the TRTs themselves can be greatly affected depending on whether it is an end-user or an institutional TRT.

Several open questions remain for this research. For future work, we will more explicitly compare end-user and institutional TRTs. We plan to deploy two user studies on two different technologies using the same study design and analysis methods. The first study will gauge people's understanding of and attitudes towards Bluetooth tracking and recording. An individual can do this type of recording.

Therefore, we will treat this study as an example end-user technology. The other study will gauge people's understanding of and attitudes towards RFID scanners and readers. This type of tracking and recording is more typical of institutions such as companies or schools. We will treat the latter study as an example of institutional technology. Explicitly comparing the two will show where the two categories of technologies are the same and where they differ. This comparison will hopefully contribute insights into attitudes surrounding these technologies that may support the design, deployment, and adoption of new TRTs.

Ackowledgments A US Department of Education GAANN Fellowship to the first author has supported this research. We would like to thank Don Patterson and David Redmiles for their helpful comments and feedback on previous drafts of this paper. Additionally, we would like to thank Khai N. Truong, Charlotte P. Lee, Alfred Kobsa, Sameer Patil, Yang Wang, Daniel Avrahami, Joe Tullio, Jennifer Rode, Amanda Williams, Elaine Huang, and Richard Beckwith for their input and comments surrounding this research.

References

1. Abowd GD, Mynatt ED (2000) Charting past, present, and future research in ubiquitous computing. ACM Trans Comp Hum Interact 7(1):29–58
2. Beckmann C, Consolvo S, LaMarca A (2004) Some assembly required: supporting end-user sensor installation in domestic ubiquitous computing environments. Paper presented at UbiComp 2004: ubiquitous computing
3. Beckwith R (2003) Designing for ubiquity: the perception of privacy IEEE Pervasive Comput 2:40–46
4. Beckwith R, Mainwaring S (2005) Privacy: personal information, threats, and technologies. Paper presented at the 2005 international symposium on technology and society. ISTAS 2005. Weapons and wires: prevention and safety in a time of fear
5. Berger PL, Luckmann T (1967) The social construction of reality: a treatise in the sociology of knowledge. Anchor Publishing, New York
6. Boslau M, Lietke BC (2006) RFID is in the eye of the consumer—survey results and implications. Marketing from the trenches: perspectives on the road ahead, pp 1–19
7. Brotherton JA, Abowd GD (2004) Lessons learned from eClass: assessing automated capture and access in the classroom. ACM Trans Comp Hum Interact 11(2):121–155
8. Brown B, Taylor A, Izadi S, Sellen A, Kaye J, Eardley R (2007) Locating family values: a field trial of the whereabouts clock. Paper presented at the UbiComp 2007: ubiquitous computing
9. Capgemini (2004) RFID and consumers: understanding their mindset
10. Consolvo S, Rode JA, McDonald D, Riley C (2005) Developing privacy personas: handling inconsistencies in attitudes & behaviors: Intel Research Seattle Tech Report
11. Crovitz LG (2008) Privacy? We got over it. Wall St J. http://online.wsj.com/article/SB121962391804567765.html
12. Goffman E (1959) The presentation of self in everyday life. Anchor Books, New York
13. Goffman E (1967) On face-work: an analysis of ritual elements in social interaction interaction ritual—essays on face-to-face behavior. Pantheon, New York
14. Hayes GR (2007) Documenting and understanding everyday activities through the selective archiving of live experiences. Doctoral thesis, Georgia Institute of Technology, Atlanta
15. Hayes GR, Gardere LM, Abowd GD, Truong KN (2008) CareLog: a selective archiving tool for behavior management in schools. Paper presented at the sigchi conference on human factors in computing systems (CHI 2008)
16. Hayes GR, Kientz JA, Truong KN, White DR, Abowd GD, Pering T (2004) Designing capture applications to support the education of children with autism. Paper presented at the UbiComp 2004: ubiquitous computing
17. Hayes GR, Patel SN, Truong KN, Iachello G, Kientz JA, Farmer R et al (2004) The personal audio loop: designing a ubiquitous audio-based memory aid. Paper presented at the mobile human-computer interaction—MobileHCI 2004
18. Hayes GR, Poole ES, Iachello G, Patel SN, Grimes A, Abowd GD et al (2007) Physical, social, and experiential knowledge in pervasive computing environments. IEEE Pervasive Comput 6(4):56–63
19. Hayes GR, Truong KN (2009) Selective archiving: a model for privacy sensitive capture and access technologies. Andrew Senior (ed) Protecting Privacy in Video Surveillance (to appear) (forthcoming)
20. Honess T, Charman E (1992) Closed circuit television in public places. Police research group crime prevention series paper 35, HMSO
21. Iachello G (2006) Privacy and proportionality.Doctoral thesis, Georgia Institute of Technology, Atlanta
22. Jancke G, Venolia GD, Grudin J, Cadiz JJ, Gupta A (2001) Linking public spaces: technical and social issues. Paper presented at the proceedings of the SIGCHI conference on human factors in computing systems (CHI 2001)
23. Jensen C, Potts C, Jensen C (2005) Privacy practices of Internet users: self-reports versus observed behavior. Int J Hum Comp Stud 63(1–2):203–227
24. Karas S (2002) Enhancing the privacy discourse: consumer information gathering as surveillance. J Technol Law Policy 7:29. Available at SSRN: http://ssrn.com/abstract=301904
25. Kumagai J, Cherry S (2004) Sensors and sensibility. IEEE Spectr 41(7):22–28. doi:10.1109/MSPEC.2004.1309801
26. Levine M (2000) SIDE and closed circuit television (CCTV): exploring surveillance in public space. In: Postmes T, Spears R, Lea M, Reicher S (eds): SIDE issues centre-stage: recent developments in studies of deindividuation in groups. Royal Netherlands Academy of Arts and Sciences, Amsterdam
27. Lucky RW (2008) Zero privacy. IEEE Spectr 45(7)
28. Lyon D (2001) Surveillance society: monitoring everyday life: Open University Press, Buckingham
29. McCarthy JF, Anagnost TD (1998) MusicFX: an arbiter of group preferences for computer supported collaborative workouts. Paper presented at the ACM conference on computer supported cooperative work
30. McCullagh D (2004) Database nation: the upside of "zero privacy". Reason
31. Mynatt ED, Rowan J, Craighill S, Jacobs A (2001) Digital family portraits: supporting peace of mind for extended family members. Paper presented at the SIGCHI conference on human factors in computing systems (CHI 2001)

32. Newswire I (2004) Grocery store loyalty card use is strong despite privacy concerns
33. Palen L, Dourish P (2003) Unpacking "privacy" for a networked world. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems (CHI 2003)
34. Patil S, Kobsa A (2005) Uncovering privacy attitudes and practices in instant messaging. Paper presented at the GROUP, ACM conference on supporting group work
35. Patterson DJ, Ding X, Noack N (2006) Nomatic: location by, for and of crowds. Paper presented at the location- and context-awareness
36. Pedersen ER, McCall K, Moran TP, Halasz FG (1993) Tivoli: an electronic whiteboard for informal workgroup meetings. Paper presented at the INTERACT '93 and CHI '93 conference on human factors in computing systems
37. Salazar C (2001) Building boundaries and negotiating work at home. Paper presented at the 2001 international ACM SIGGROUP conference on supporting group work
38. Schilit B, Adams N, Want R (1994) Context-aware computing applications. Paper presented at the IEEE workshop on mobile computing systems and applications
39. Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly 20(2):167–196
40. Solove DJ (2007) 'I've got nothing to hide' and other misunderstandings of privacy. San Diego law review, 44
41. Spiekermann S (2007) Privacy enhancing technologies for RFID in retail—an empirical investigation. Paper presented at the UbiComp 2007: ubiquitous computing
42. Strauss AL, Corbin JM (1998) Basics of qualitative research: techniques and procedures for developing grounded theory. Sage Publications, Thousand Oaks
43. Sudman S, Bradburn NM (1982) Asking questions: a practical guide to questionnaire design. Jossey-Bass, San Francisco
44. Truong K, Abowd G, Brotherton J (2001) Who, what, when, where, how: design issues of capture & access applications. Paper presented at the Ubicomp 2001: ubiquitous computing
45. van de Garde-Perik E, Markopoulos P, de Ruyter B, Eggen B, Ijsselsteijn W (2008) Investigating privacy attitudes and behavior in relation to personalization. Social Sci Comp Rev 26(1):20–43
46. Want R, Hopper A, Falc V, Gibbons J (1992) The active badge location system. ACM Trans Inform Syst 10(1):91–102
47. Want R (2004) RFID: a key to automating everything. Sci Am 290(1):56–65
48. Weiser M (1991) The computer for the 21st century. Sci Am
49. Zureik E, Harling-Stalker L, Smith E, Lyon D, Chan YE (2009) Privacy, surveillance and the globalization of personal information: international comparisons. McGill-Queen's University Press, Kingston (forthcoming)