Situated Privacies: Do you know where your mother [trucker] is?

Ken Anderson

Intel Research
Intel Corporation
2111 NE 25th Ave, MS:JF3-377
Hillsboro, OR 97124/USA
ken.anderson@intel.com

Paul Dourish

Donald Bern School of Information and Computer Sciences
University of California, Irvine
Irvine, CA 92687
jpd@ics.uci.edu

Abstract

We describe the privacy practices of long haul truckers and members of an assisted living center. We conclude that conventional interpretations of privacy, namely, cost/benefit trade-offs of information exchange, don't take into account a critically important set of social issues that arise in real-life settings. The social-cultural practices within which information is embedded give meaning not just to information but to the ways in which it is used. We conclude that "privacy" is not the primary issue. Instead, the issues are how groups of people choose to share or not to share, or not to notice information. As a means towards a more effective understanding of the relationship between people, information, and technology, we advocate using an ethnographic approach to understand the social contests and collectives within which discursive practices occur. By taking these perspectives, we hope for a better understanding of the relationship between people, technology and practice, and provide a firmer foundation for developing technologies that can be incorporated into everyday information practices.

1 Introduction

In the late 90's, none of my work colleagues knew how much anyone else made; this information was considered highly private. At the same time in Norway, everyone's salaries were considered public information, and indeed were published. That cultures would have different constructs of "privacies" should come as no surprise (Culnan and Armstrong 1999). The cross-cultural understanding of privacies, therefore, provides fertile ground for anthropologists and computer scientist, and is critical as the world moves ever further into the information age. In contrast to others who have looked at privacy practices on a national scale (e.g., nation-states like Norway and the USA), we explore the ways in which small collectives affect privacy practices. Examining privacies that arise out of such smaller collectives offers a way for technology design to succeed in the development of systems that bridge the relationship between the individual, technology systems and cultural practices. Beliefs and practices around privacy are not limited solely to a mobile phone or a computer, but rather the technologies are sites of meaning production that are implicit in broader social-cultural issues around collective and personal identity, as well as power.

Here, we describe the privacy practices of two small collectives: an assisted living community and long haul truckers. We conclude that conventional interpretations of privacy, namely, cost/benefit trade-offs of information exchange, don't take into account a critically important set of social issues that arise in real-life settings. The social-cultural practices within which information is embedded give meaning not just to information but to the ways in which it is used. Since technologies are situated in sites of social and cultural production, technologies reinforce social and cultural power relationships. Further, notions of private and public imply differences in beliefs and practices. We argue that these differences are not taxonomic, or categorical, but interactive and refractive. The "interactive" nature of privacy, or information in general, is not idiosyncratic, but a pervasive social-cultural linguistic act. We argue that an ethnographic approach to privacy provides a valuable methodology for investigating this socio-technical nexus.

Our original inquiry was not about "privacy" *per se*, but about how groups of people engage in sharing, not sharing, and not noticing information; in choosing to share, not to share, or not to notice information; and in being seen to choose to share, not to share, or not to notice information. As a means towards a more effective understanding

between the relationship between people, information, and technology, we advocate an approach that is not based on abstract taxonomic ideas of private/public, but rather on empirically evident "information practices" and "privacies." We need to look not only at information flows, but at what social ends are achieved through those flows. By taking these perspectives, we hope for a better understanding of the relationship between culture, people, technology and practice, and provide a firmer foundation for developing technologies that can be incorporated into everyday information practices.

2 Background and Approach

Here, we describe two ethnographic investigations of emerging practices of privacy with information technologies among two disparate small collectives: among the residents of an assisted living facility, and among long haul truckers. These two studies have informed our thinking about approaches to privacies as discursive practice. We argue that the we, the community of researchers interested in privacy issues related to technology, need to expand our thinking beyond taxonomic approaches. If we do not "widen our nets," we are likely to misconstrue the problem, and as a consequence, to misinform. Discursive practice is based on approaching technologies as socially constructed and culturally embedded objects; technologies are not neutral. Further, notions of "public" and "private" are not rigid taxonomic categorizations, or even necessarily cross-culturally relevant categories. Finally, privacy cannot be approached in purely economic terms, but should be approached as a collective practice. While it may be said that the concept of privacy is of social origin (Weinrich and Sasse, 2001; Palen and Dourish, 2003), for us what is of interest is the exploration into the nature and scope of this social origin.

2.1 "Private" and "Public" Situated Concepts

Traditionally, we as a field, have postulated two realms of information, "private" and "public." This distinction helps to simplify building systems that erect and maintain barriers between these two. These studies fail to account for technologies as sites of social and cultural production. The result is a loss in the understanding of cultural richness and social complexity of real deployment situations. Palen and Dourish (2003) adopted Irwin Altman's (1975) approach to privacy as a continuous, dynamic and dialectic process of boundary regulation. The argument is that the boundaries between public and private are not fixed but are continuously renegotiated in interactions. Palen and Dourish map out a number of boundaries as part of the privacy process, like privacy/publicity, self/other, past/present/future, in order to explore problems associated with a range of technologies. This work matches closely with Nippert-Eng's (in press) study of boundaries of privacy/publicity. Although these approaches are a leap forward in privacy studies, they retain a primary focus on the ways in which activities are labelled as private and public rather than on the practices through which not just one but many forms of "privacies" are enacted in the course of participation in a range of social groups.

Schegloff's (1972) work on place provides and insightful model of the negotiation of privacy. Schegloff has noted how location descriptions and directions follow the relationship a person has with the interactor with whom they are interacting at a given time. The relationship is not necessarily static, but are contingent upon the situation at-hand. Often the relationship is not known, but is negotiated through the interaction. As a default starting point in location conversations the default is to approach the interactor as a "stranger." What is interesting for us, is that like location, practices around privacy follow similar interactional rules. The first step in the interaction is to differentiate between known and unknown interactors. Once this is established, what becomes key is differentiating between classes of known and unknown sources, e.g. core family, extended family, intimate friends, acquaintances, members of the same gym, etc. The context of the interaction then is in part based on the collective values, beliefs and practices around privacy. In Muslim communities, for example, gender differentiation is crucial. A problem for system design, however, is that individuals are clearly part of many collectives at the same time. Indeed, as a part of a communicative event, it becomes important to note context of communication. Hymes (1974) has outlined key aspects of the communicative action as setting, message form, message content, scene, speaker, addressor, hearer, addressee, purpose-outcome, purpose-goal, key, channels, forms of speech, norms of interpretation, and genres of the speech community. These are helpful guidelines for design research into the collective nature of privacy. The primary question for both Hymes and Schegloff pertains to which "speech community" is under discussion. Indeed, the collective where the technology is going to be deployed needs to be identified.

2.2 Privacy as economic rationality

Most discussions of privacy adopt, either explicitly or implicitly, an approach that we will refer to as an economic model. This is not to imply that it is financial; rather, it is economic in the sense that the central element of this approach is the idea of a trade-off between risk and reward, the cost and benefit associated with sharing, revealing, or transmitting information. Information is modelled as a commodity that can be traded. Discussions of credit card use, for example, regularly turn on the idea that the benefit that people gain from being able to charge purchases conveniently outweighs the potential costs of making information about purchase history available to the credit card company; similar arguments apply to situations as diverse as store loyalty cards and presence availability in Instant Messaging (Patil and Lai, 2005). We refer to this as an economic model because of its fundamental reliance on two concepts. The first is the concept of exchange value; this model implies both that information is traded for benefit, and that items of information can be compared and ordered by their exchange values. The second is the figure of the rational actor, the user who assesses current and potential future situations and calculates their costs and impacts. The economic approach to privacy models collective action as the outcome of individual decision-making by rational actors optimizing for individual benefit.

The economic model is the assumed model of many proposals around ubiquitous computing. For instance, Intel's Place Lab (Schilit et. al., 2003) offers a platform for location-based services. The framework provides the users with control over the ways in which their location is disclosed (Hong et. al., 2003). The system uses a Place Bar, which allows users some degree of control over specificity with which their location is reported, for example a zoom control like make Mapquest (www.mapquest.com) that moves from room, to building, to street, to city level. The notion of rational choice and exchange is explicit in this structure. Similar approaches have been used in k-anonymous location systems (Grusteser and Grunwald, 2003) or RFID in retail applications (Floerkemeir et. al., 2004).

2.2.1 Collective Discursive Practice as a Critique of Economic Model

The economic model, or rational actor model is intrinsically appealing but lacks power as the sole explanatory force. Recent research has shown how this approach fails to account for everyday behaviour, as wall as highlighting social factors interfere with neoclassical economics (Rabin, 1998 Kahneman and Tversky 1979) We suggest, however, that the economic model fails to recognize that privacy and information practices are primarily social practices. Economic models may provide a quick gloss of information practices, however, as Giddens (1993) and similarly Mauss (2000) point out, all "social action" is multidimensional; it is at once a "social act," an "economic act," a "political act," and "interpretive act." The focus solely on the economic is covering only part of the needed explanation for effective system design. Thus, the "interpretive" or "signification" strand of the "social act" is what makes the "social act" both generally (say "culture") and specifically (say "symbolic interaction") "meaningful." In other words, Giddens categorically denies the idea that there can be some foundational "political act," or "economic act," precisely because these are always meaningful and interpretable to participants and, therefore, fundamentally cultural.

Furthermore, Giddens rejects the idea that either "culture" or "social structure" are static, permanent, monolithic structures that are just "out there," or, for that matter, just in people's heads either. Interaction is what constitutes "structure," but it does not do this predictably because interaction can, in principle, result in a change in the rules, even if we find, as an empirical matter, that more often than not interaction simply reproduces and reaffirms what "everyone always knew anyway." Giddens insists that signification, domination and allocation are intricately intertwined (empirically inseparable) dimensions of social interaction, the production/reproduction/transformation of "structure." In this way we can think of privacy as a discursive phenomenon. By this we mean to draw attention to privacy as aspects of *communicative* and *linguistics* practice of a collective. It is through the social use of language and interaction that we shape and constitute the world that we experience.

Language always embodies a particular perspective and understandings about power. In the case of privacy these perspectives and understanding of power relations are embodied in the questions: Privacy for whom? Privacy of what ? Privacy from whom? And who gets to define them? The discursive practices reflect and reinforce power relations and conceptual models. Agre (1995) has note how in discussing privacy problems, designers often frame the problem not as the potential loss of privacy that people might experience, but rather as the potential rejection of the technology. We can easily see similar problems in discussion around privacy and surveillance. When appeals to the right of privacy are met with a rejoinder that "people who have nothing to hide have nothing to fear," a rhetorical

move has turned questions of privacy into questions of secrecy. Warren and Laslett (1977) point out that while privacy is an acknowledged right in the West, there is no right to secrecy.

3 Field Studies

We selected our particular field sites because of the relatively recent introduction of new location monitoring technologies to the respective communities. In communities, after some time, norms and even laws appear around what is considered to appropriate behaviours. In the USA, for example, it is illegal to record a phone conversation or even a conversation in public without the acknowledged consent of the other person, or a legal writ. In most communities there are emergent community standards, however, when technologies are new to a community; social practices are not yet fully developed around them. Reed (in press) describes how early bloggers in London were shocked to find their blogs read by family and friends. They felt their privacy had been invaded. In March of 2004 David Beckham was caught off guard when what he thought were private ephemeral SMS messages between him and his assistant, whom he was allegedly have an affair, were printed in the London papers (Mirror 2004). Cases like these help to identify areas were technology and social practices meet, and sometimes collide. These instances not only help us identify the process of adoption but also where and how social practices occur in collectives.

3.1 Ben Fica Assisted Living Community

3.1.1 Background and Setting

Ben Fica Estates is a privately owned assisted living facility. It consists of a small campus (about 5 acres) in a suburban area. When we conducted our 3 month-long study in one residential facility, Mountain View. The campus consisted of 5 houses and a central operations building. The houses contain residential apartments (with a maximium number of residents 15), shared rooms in residential homes include a living room, great room, and greenhouse. The private apartments had a bed space, a bathroom, and a small common space. The individual units did not contain any kitchen facilities. The buildings do not have any hallways, which might hinder access to the common areas. Each residence hall has two stories, plus a daylight basement. The residents shared all meals together, as well as, snacks. The apartments were designed for occupation by single individuals or couples. An on-site resident assistant lived in the basement apartment, where there was also a laundry facility. The 5 buildings formed a perimeter for the campus, with a central area designed with gardens and parking. Residents were free to wander the campus and be involved with many “community” activities.

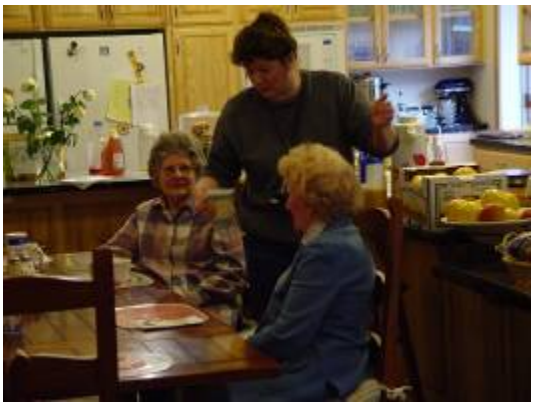
Technically, Ben Fica was designed to support ubiquitous computing. At the time of our study, there were programmable logic controllers for lighting, overhead fans, heating, ventilation and air conditioning. Further, each door had switches on it noting the state of the door (open/closed) that were continuously monitored. Motion sensors were place in both public spaces and private residences to monitor movement in each room. Load cells were on the beds of the residents that monitor the weight, and by inference, movement in the bed. Finally, every resident and worker wore badges with unique IDs. Badges broadcasted the specific ID of the person both in IR and RF for location monitoring. Badges for residents also included a call button that sent a signal in both IR and RF when assistance was required. The location of residents and workers was available on 12 inch PC monitor in central room of each building, as well as, in the office building. Not one of the residents used the monitor during our observations. The staff of the house looked at the screen only 9 times during the 3 month observational period. One of the difficulties with the public display of information was that the screen refreshed the more than 48 names every 10 seconds. When the staff did use the location information on the screen, they had to watch it refresh for over a minute to locate the name and the location, since these were reported as they came into the server, not alphabetically or by house. The Ben Fica staff manager routinely checked the location monitoring screen, at least twice, every time she visited the house (which was at least once a day).

3.1.2 Privacy Method

This study, and another reported in Beckwith and Lederer (2003) focus on privacy in assisted living communities. One of the first issues encountered, even in this heavily instrumented environment, was a methodological one around interviewing. Asking directly about privacy, either in terms of practices, places and objects, yielded what at first were unsatisfactory results. People had difficulty labelling in the abstract activities, objects, information and places as either public or private. The failure to categorize information easily was actually important, as we learned over time. The dining area was used for community gatherings but also sharing moments of closeness and confidence between people. The dining area/great room was constantly referred to as a public space with public activities, yet in behaviours it was full of intimate and private moments. Information, too, had shifting value and practices. Gossip about residence, their families, staff and management filled many conversations. Gossip had a certain social value. There was good gossip and bad gossip. As a discursive practice, the gossip about "private" and "secret" information had social values and appropriate practices associated with it. The point is it would be hard to pre-program a place or set of information around single variables or even "averaged" behaviours. Nor, often, would a speech event actually to able to be labelled as public/private until after it had occurred. It is not that these events are about boundary management (between public and private) but about boundary management of belonging and not belonging, about identity and reputation management.

3.1.3 Not So Candid Camera

The technology describes what was in place when we arrived for this part of the study. Earlier the management at Ben Fica had put a camera pointed at the dining room space in each of the resident buildings. The management idea was that families could "peek" in on their relative. Further, it was thought that it would create a better sense of community if each of the facilities could see what was happening in the other buildings, so while they were physically separated they could visually be in view. The cameras were mounted unobtrusively on the walls.



The cameras were gone within a week. Residents and their family asked that they be removed. Margaret, one of the residents, described to us how she felt "watched, like someone was peeking over my shoulder all the time." Ethel, another resident, talked about the camera as "window without curtains on my dining room," anyone could see in. Upon investigating further, the being watched was serious problem. Residents come into the dining area sometimes in very casual clothes, like a robe, pyjamas and slippers. While we were there, the residents only commented upon the dress of others when they looked particularly "dressed up," often as a linguistic opening to see if they were going out for the day. The information not "noted" was when people looked dishevelled, like they just woke up, or were in their pyjamas. With the cameras, there was a sense as Ruth described it that "we are on TV." The dining space that had come through practice to be labelled as private for the house, was now open to others (public). The residents, along with their families, rebelled.

The activities that residents engaged in the space were also not particularly "the best" side of residents. Eating was often messy for some of the residents. Conversations were not always harmonious, since house members did not necessarily get along all the time. On Thursday as lunch was being set up, a resident came in from the elevator singing and then said to another resident, "you're disgusting." She responds, "disgusted or disgusting?" He says, "Both!" In short, the residents wanted to keep these behaviours taking place in the public space of the residence to be kept private from those outside of the physical community. In terms of location awareness, it is one thing to know where someone is, it is another thing to know what they are doing. Locations around the campus, for the most part, were not given any particular value. Actual activities, on the other hand, were often observed by those present, but not meant to go beyond that group.

3.1.4 Management Panopticon

The location practices of those immediately involved in the community varied. We'd first like to discuss management's perceptions of location tracking. We are defining management here as those whose job function was

not directly tied to the day-to-day care of residents. The location monitoring system was considered a key feature in the distinctiveness of Ben Fica as an assisted care facility. Bob, one of the owners stated, "We can let the family of our residents always know where their loved ones are, that is a comfort to them. It shows we care." On another occasion, he commented, " We can provide a sense of security to the family that someone is watching over their parent or grandparent at all times." Betsy, his wife, "'Did my mom get out today?' is a question we are constantly asked – well, I can tell them 'yes' because we have tracking data from the day that I can look at . . . neither me or the family has to rely on what workers report; we have the actual data right here." "We have a large campus. When a family member or someone arrives unexpectedly, we can find the residents instantly for them . . . What a benefit that is . . . *residents are able to look and feel free but we can always find them*. Indeed an instrumental value of the system was letting the office monitor location of all residents for the reassurance of their families.

Residents are not the only ones tracked, "We track our employees too . . . Eventually we hope to bill for extra services or time they spend with the residents," explained Betsy. As time passed, we heard other sides of the story from Bob, "A huge problem in our industry is getting the right kind of help. We pay a higher hourly than most [assisted living facilities] but that doesn't guarantee the right kind of person gets hired. There are not a lot of PhDs knocking on our doors looking for work. . . . The badge *at least* lets us monitor that our workers are spending time with our residents." Bob, the owner, asked Elizabeth the head staff person of Mountain View residence, "why do you spend an hour in the bathroom every morning? Bob apparently wasn't aware that the bathroom on the floor had been converted to a medical dispensing room, where Elizabeth was sorting medication. But the point was the staff were made aware that their movements were observed through this system, with the potential for reprimands and termination. Location did not, however, tell what activity was happening, only the location of the badge. Staff members would take the badges off and hang them on chairs of residents to go out for a smoke or a breath of fresh air. Since some resident was almost always in watching TV, this wasn't very difficult. Residents would also sometimes just volunteer to take the staffer's badge. I asked one of the residents about holding the badge for one of the staff people. She responded, "Well, Stacy is just such a hard worker. . . . She helps me when I have problems with wetting my bed, and cleaned up and keeping me looking good. It is a lot of hard work. Every once-in-awhile the girls just need to take some time out for themselves. With all of us here, we always keep them really busy, because I'm one of the easy people! . . . We put a lot of demands on them (the workers), this is just a little thing I can do." Of note here, was the resident's desire to have a sense of partnership, of belonging and identifying with the staff. The other point we wanted to make, however, is that system was really designed to support the power structure that already existed. The stated intent at the development was to help residents and families be sure of high quality care, yet the resulting practices reinforced beliefs and practices by both staff and management that had long been in place.

The staff supervisor wore a badge but many of the other people in the office context did not regularly wear them. Indeed, one of the issues with the house workers was they could not find office staff when they needed them. The relationship was not equal. Here the community practices that were in place before the technology are only more strongly reified in the technology of tracking. The tracking system was not infallible either, and staff and residents used this plausible deniability tact on more than a few occasions. During one 8-hour day, the systems had at least 9 false reads, though on others it had none that we knew about. Staff knew where the residents of their buildings were at all times without the tracking, by simple visual monitoring of the building and the grounds. Management, however, would make check ups on staff. The staff could respond with "I was working cleaning up Bonnie, didn't my badge show that?" while they might really be somewhere else. The problem for management was when family members or healthcare professional might arrive, and not have the correct location of the resident.

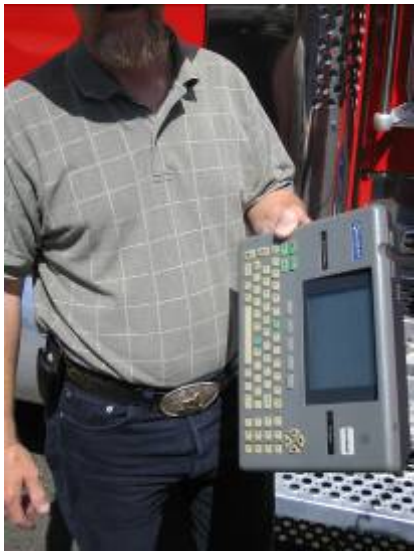
3.1.5 The Magic of Invisible Information

We've discussed a lot about what people in the community were noticing, however, discursive practice can involve not noticing. Whorf (1956) noted this in terms language. In one of his incident reports, an employee who had placed drums of gas near a heater, believed that although a 'flammable' liquid would burn, something as inflammable as a steel drums, would not. The risk to him was mediated by the language, which was intimately link to society's beliefs. Goffman (1965) has noted a similar information practice around "civil inattention." We see in this collective practices that developed around not noticing information. Besides the location sensors for residence, we mentioned that the facility had attached load sensors to the seniors' beds to track their weight and sleep restfulness for health reasons. However, the information gathered and reported to family members could also indicate that the senior was

sleeping with/dating someone (and, through the use of badges, could potentially specify with whom). Family members and residents were upset with the management for disclosing this information. The information about sleep restfulness is still collected and reported, however, no one "sees" the information about bedroom partners; it became invisible information. This was in essence both a collective decision as well as one that reflected the power dynamics at work (since the family members typically are responsible for paying the bills, and so hold ultimate power). In fact, not seeing sleeping/dating partners was a return to a previously agreed-upon information practice of the residents and staff from a time before the technologies were deployed. Indeed, it was not new information for service people for they had always negotiated out as a part of the community information practices "not to see it." It was agreed upon invisible information, a "safe" behaviour in that context.

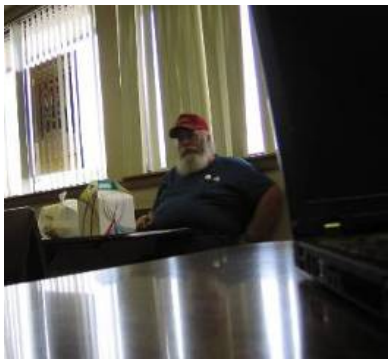
3.2 Long Haul Truckers

"Now, what would you do if that minivan would suddenly come to a stop or spin? You'd have two choices: (1) you can run over that minivan with this rig, killing that mom and all those kids or (2) you can drive off the freeway into that cement barrier killing yourself. What are you going to choose to do in that split second. . . . Real long haul truckers know that there can be a situation like this at anytime. They are prepared for it. A trucker wouldn't even hesitate, they would choose to die themselves rather than killing a motorist." This was one of the many situations Stan, a long haul driver now for 24 years, had discussed with me about who is a long haul trucker and who is not. "Everyone who drives a truck isn't automatically a long haul trucker, you have to learn how to be one," Tammy and Jim (a couple who had been driving now for 3 years) explained over coffee. They felt just this year that they had really become long haul truckers. There are several characteristics of belonging that were easy to articulate but others were more part of everyday practice. Practices around what information to share, when to share, how to share or not share are also part of being a long haul trucker.



3.2.1 Technology Context

Many independent truckers end up driving for companies that use a satellite tracking system on the cabs and/or on the trailers. The system consists of an antenna on the roof and a tablet like device in the cab. The truckers attributed the need for the tracking system to new drivers who may try to get jobs just to steal loads, "you can't trust just anyone who drives a truck." In this study we conducted contextual interviews with 25 truck drivers over a month long period. We were researching technology uses by long haul truckers. In particular, we focused on truckers with these tracking systems in place, with some additional interviews with other long haul truckers for comparison. We met the truckers at truck stops in Washington and Oregon. Two of the key points for truckers in discussing their community of practice were information about routes to take and how to get a load for the return trip. Each of these draws on information and privacy practices.



As people became truckers, they would learn from other truckers the "secrets" of running with heavy loads, driving longer hours, temporarily disabling GPS cab monitors, and navigating effectively and cheaply with wide loads. The "secrets" of the trade were not just revealed to anyone, but over time as truckers talked with each they could assess the other driver – who did they know, what do they drive, how long have they been driving, how did they handle their last route, etc. Collective information practices also dictate what is not to be shared. For example, asking a trucker for a contact in a city to get a return load, or for a password to a web site that provides return loads, is extremely inappropriate. In truck stops where a trucker would be using a laptop, other truckers coming into the space would go to great lengths to avoid looking at the screen until they had probed to be sure that the trucker wasn't working to find a load. The truckers didn't want to be perceived as violating community conventions about work. On another occasion, however, I was with a trucker who was explaining to a driver new to the satellite tracking systems that it does "just go out of

alignment." "You need to bring yourself back into alignment by pointing your truck South, toward Texas. The satellite rotates along there. . . . I call it praying to Texas 'cause you can't see anything but then magic happens with your tracking gear. . . . You can also take advantage of this by telling the dispatcher that you were en-route and driving or not driving but must have not been in alignment with that satellite. It must be some technical error. You can't do it much but it is good to know when you need to use it." Again, truckers have collective, normative information practices that define and mark them as a collective. As part of the process of enculturation, new members must learn what sort of information is to be shared and what not, and must develop new understandings of the norms that govern information use.

4 Conclusion

Understanding and designing for privacies as part of a technology system is a complex process. Technological innovation is moving into a greater variety of social contexts with a range of devices. Indeed, mobile phones are pervasive, as are the use of voice, SMS, cameras/photos, GPS and e-mail on them. As technologies capture more of our personal and collective contexts a key concern will be about privacy practices. We join technology designers and developers who recognize that privacy concerns are not something that can be retrofitted to technologies, but should be integrated into system, structure and usage models. We believe that approaching the discursive practices of collectives around information will be a fruitful direction for exploration and system development. Technology concerns then are with collective information practices. We have demonstrated that collectives, through strategic use of information, use technology as a site of cultural and social production. In short, the technologies are not the ends, but are a platform in which people engage in social action. It is not what people mark as private, but how can we enable users to strategically deploy information of all kinds. There should be no normative distinctions "built in" about private/not private; it is not up to designers, only the users can define these. As we have seen information is shared for a variety of reasons. Technology can't distinguish between social states; technology can only distinguish technological states. We urge developers to give people the technological resources they need to make the distinction. Privacy and publicity are forms of collective information practice. We need to concern ourselves with how we can build technological support for public and private practices that people want to engage in.

Our recommendations are as follows:

- Understand privacy as a discursive practice.
- Public/private does imply difference, but the differences are not taxonomic; they are interactive and refractive.
- Explore and represent collective discursive practices using ethnographic approaches.
- Technologies often mirror and reproduce the articulated and unarticulated social/political relations.
  - Who gets to define what is private, secret, risky, public, shared is a key issue.
- Privacy is part of a set of information practices cannot be separated from other information practices, like identity, and community that collectively give them meaning.
- Technologies need to be conceived of as platforms for social practices.

References

Agre, P. (1995). Conceptions of the User in Computer Systems Design. In Thomas (ed), The Social and Interactional Dimensions of Human-Computer Interfaces. Cambridge University Press.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? Journal of Social Issues, 13(3), 66-84.

Beckwith, R. and Lederer, S. (2003) Designing for One's Dotage: Ubicomp and Residential Care Facilities, Conference on the Networked Home and the Home of the Future (HOIT 2003), Irvine, CA: April 2003.

Culnan, M.J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104-115.

Cummins, F, and S. Moyes (2004) Beckham's Raunchy Text Sex, Mirror. March 5.

Floerkemeier, C., Schneider, R., and Langheinrich, M. (2004). Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols. Proc. Second International Symposium on Ubiquitous Computing Systems UCS 2004 (Tokyo, Japan).

Giddens, A (1993) New Rules of Sociological Method: A Positive Critique of Interpretative Sociologies. Stanford: Stanford University Press.

Giddens, A (1991). Modernity and Self-Identity: Self and Society in the Late Modern Age. Stanford: Stanford University Press.

Goffman, E. (1966). Behavior in Public Places. New York: The Free Press.

Gruteser, M. and Grunwald, D. (2003). Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. Proc. ACM/USENIX International Conference on Mobile Systems, Applications and Services (Mobisys 2003).

Hymes, D. (1974). Foundations in Sociolinguistics: An Ethnographic Approach. Philadelphia: Univ of Philadelphia Press.

Kahneman, D. and Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. Econometrica, 47(2), 263-292.

Mauss. M. (2000) The Gift: The Form and Reason for Exchange in Archaic Societies. London: W. W. Norton and Company.

Nippert-Eng, C. (in press). Disclosure and Concealment: Privacy, Identity Work and the Use of Wallets and Purses.

Palen, L. and Dourish, P. (2003). Unpacking "Privacy" for a Networked World. Proc. ACM Conf. Human Factors in Computing Systems CHI 2003 (Ft Lauderdale, FL). New York: ACM.

Patil, S. and Lai, J. (2005) Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application for a Networked World. Proc. ACM Conf. CHI 2005 (Portland, OR). New York: ACM

Rabin, M. (1998.) Psychology and Economics. Journal Of Economic Literature, 36, 11-46.

Reed, A. (in press) Blogger.

Schegloff, E. (1972) Notes on Convesrsational Practice: Formulating Place in Studies in Social Interaction, D. Sundlow (ed) NewYork: The Free Press.

Schilit, B., LaMarca, A., Borriello, G., Griswold, W., McDonald, D., Lazowska, E., Balachandran, A., Hong, J., and Iverson, V. (2003). Challenge: Ubiquitous Location-Aware Computing and the "Place Lab" Initiative. Proc. ACM Intl. Workshop on Wireless Mobile Applications and Services on WLAN (San Diego, CA).

Warren, C. and Laslett, B. (1977). Privacy and Secrecy: A Conceptual Comparison. Journal of Social Issues, 33(3), 43-51.

Weirich, D. and Sasse, A. (2002). Pretty Good Persuasion: Steps Towards Effective Password Security in the Real World. Proc. ACM New Security Paradigms Workshop, 137-143.

Whorf, B. (1956) Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf. , J. Carroll (ed) .Cambridge: MIT Press.