

Location Disclosure to Social Relations: Why, When, & What People Want to Share

Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge

Intel Research Seattle

1100 NE 45th Street, 6th Floor, Seattle, WA 98105

[sunny.consolvo, ian.e.smith, anthony.lamarca, pauline.s.powledge]@intel.com,
tmatthews@cs.berkeley.edu, jrtabert@u.washington.edu

ABSTRACT

Advances in location-enhanced technology are making it easier for us to be located by others. These new technologies present a difficult privacy tradeoff, as disclosing one's location to another person or service could be risky, yet valuable. To explore whether and what users are willing to disclose about their location to social relations, we conducted a three-phased formative study. Our results show that the most important factors were *who* was requesting, *why* the requester wanted the participant's location, and *what* level of detail would be most useful to the requester. After determining these, participants were typically willing to disclose either the most useful detail or nothing about their location. From our findings, we reflect on the decision process for location disclosure. With these results, we hope to influence the design of future location-enhanced applications and services.

ACM Classification Keywords

H.5.3. [Information Interfaces and Presentation]: Group and Organization Interfaces – evaluation/methodology, computer-supported cooperative work; H.5.2. [Information Interfaces and Presentation]: User Interfaces – evaluation/methodology, user-centered design.

Author Keywords

Experience sampling, privacy, location-enhanced computing, ubiquitous computing, privacy classification, social relations

INTRODUCTION

Imagine that it is a Saturday afternoon in the not too distant future and your boss sends a request for your location to your mobile phone. Or perhaps the request is from your

spouse and you are at his favorite store purchasing a gift for him. How should you (or your phone) respond?

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CHI 2005, April 2–7, 2005, Portland, Oregon, USA.

Copyright 2005 ACM 1-58113-998-5/05/0004...\$5.00.

Advances in location-enhanced technology are making it easier for us to be located by others. Services such as OnStar's Driving Directions, mMode's Find Things or People Nearby, and Enhanced 911 have already brought this technology to automobiles, mobile phones, and personal digital assistants. These new technologies present a difficult privacy tradeoff, as disclosing one's location to another person or service could be risky, yet valuable. Recent investigations in location-enhanced technology have focused on software infrastructures for managing this disclosure [10,12], however little work has explored how users conceive of this disclosure or would disclose in the actual situation when they receive a request.

Accordingly, in an effort to influence the design of location-enhanced technologies, we are investigating whether and what users are willing to disclose about their current location to people they know. For example, when users are willing to disclose something about their location, do they want to disclose the exact address, a generic name for the place (*e.g.*, "home" or "work"), the name of the neighborhood, city, or something else? *What* helps users decide what to disclose? *Who* is requesting? *Where* they are when they receive a request? *What* they are doing? How they *feel*?

To explore this, we conducted a three-phased formative study with 16 non-technical participants. We employed various techniques, both in-lab and *in situ*, to uncover user concerns: two weeks of Experience Sampling where participants received hypothetical requests from people they knew, a nightly voicemail diary study, questionnaires, a privacy classification survey, exercises, and interviews. The most notable results are that:

- participants want to disclose what they think would be useful to the requester or deny the request. We saw no evidence of participants intentionally blurring their location, *i.e.*, disclosing something vague, to protect their privacy, and

- participants' privacy classification, as determined by the Westin/Harris Privacy Segmentation Model [18], was not a good predictor of how they would respond to requests for their location from social relations.

From the results, we reflect on the decision process participants went through to determine whether and what to disclose about their location to social relations. Understanding this decision process and other factors that go into their decisions could inspire the design of better location-enhanced applications and services.

In this paper, we begin by describing the study design, including details of the three phases and the participant profiles. We follow with a discussion of our key findings. We then reflect on the participants' decision process for disclosing location to social relations, discuss related work, and conclude.

STUDY DESIGN

To help us understand what is important to users when choosing whether and what to disclose about their current location to their social relations, we conducted a three-phased study in July 2004 with 16 non-technical participants in the Seattle area. In Phase 1, we investigated the structure of participants' social networks and how they thought they would use location-enhanced computing. In Phase 2, participants responded *in situ* to hypothetical requests for their location from their social relations over a 2-week period, and in Phase 3, participants reflected on their experiences in the study and their attitudes about location-enhanced computing. In this section, we describe each phase, the two location-enhanced application ideas that provided context for our explorations, and the profiles of the study participants.

Methodology for Phases 1-3

PHASE 1. Phase 1 familiarized us with the participants' backgrounds, helped us understand the structure of their social networks, and allowed us to explore what they thought would be important in deciding whether and what to disclose about their location to social relations. It was conducted in our lab, one participant at a time¹. Prior to arriving for their first session, participants completed a demographic questionnaire that included a privacy classification survey: the Westin/Harris Privacy Segmentation Model [18], sometimes called the "Westin survey." Upon arriving for Phase 1, participants signed a release form and completed exercises designed to:

- identify the people in and structure of their social network and create a "buddy list" of people with whom they might want to exchange location information,

- uncover the factors they believed would be important in deciding whether and what to disclose to specific people on their buddy list, and
- gather their initial thoughts on two proposed location-enhanced applications.

The names used for the hypothetical requests came from the "buddy list" that participants created of up to 17 people² from their social networks. We required certain social relations to be on the "buddy list" to explore commonalities in the way participants treated members of the same social group (*e.g.*, family, co-workers, *etc.*). The list included:

- spouse/significant other,
- two family members of the participant's choosing,
- manager,
- two co-workers of the participant's choosing, and
- up to 11 others from the participant's social network with whom he would want to participate in the *single-request* application described below.

Participants included an average of 14 people on this list, (the range was 8-17).

Phase 1 sessions lasted from 90-120 minutes each. Data was collected in the form of evaluator notes and materials completed by the participants.

PHASE 2. In Phase 2, Experience Sampling Method (ESM) [4,6] was used to capture participant responses to *in situ*, hypothetical requests for their location from people on the buddy lists created in Phase 1. Participants also answered a variety of ESM questions about their context at the time of each request. It was administered on Palm m500s that we provided, using software [13] for running ESM on PalmOS devices. During ESM, participants received 10 randomly timed questionnaires everyday for two weeks from 9am-9pm on weekdays and 10am-10pm on weekends. Each questionnaire was composed of several questions and took approximately 2-3 minutes to complete. Questionnaires included questions about:

- context, *e.g.*, Where are you? What are you doing? With whom are you? (Figure 1) and
- what the participant would want to disclose about his location based on a hypothetical request from a social relation on his buddy list.

The questionnaires were customized to include people, places, activities, and other contexts that were meaningful to each participant. For example, instead of asking what a participant would be willing to disclose to a request from a

¹ There were two sessions of two participants each.

² We chose 17 because it is within the range of active social relations for Westerners (typical range is 10-30 [14]), allowed for a sufficient number of hypothetical requests from each buddy list member, and kept the time to fill out the Phase 2 ESM questionnaires manageable for participants.

co-worker, “a co-worker” was substituted with a name from the participant’s buddy list that was meaningful to him.

Questions about current activities were also customized. For example, during Phase 1, a participant mentioned that she would only disclose her location to her mother when she was not drinking alcohol; her “What are you doing?” question included a “drinking alcohol” option (Figure 1).

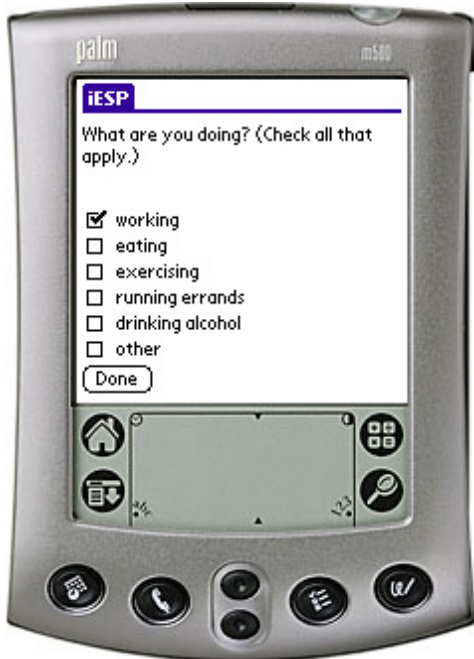


Figure 1. This ESM question asks about activity.

Participants also completed a nightly voicemail diary study to report if they went anywhere atypical for that day of the week. For example, if a participant went to the dentist one Thursday during the study, perhaps for his biannual check-up, he would report that in his voicemail diary; however, if he usually goes to the dentist on Thursdays, he would not report the visit. Data collection consisted of the ESM responses and audio recordings of the voicemail diaries.

PHASE 3. In Phase 3, participants reflected on their experiences in Phases 1 & 2, particularly their attitudes about location-enhanced computing and disclosing their location to social relations. Conducted one-on-one and in our lab, Phase 3 took place shortly after the last ESM questionnaire and consisted of several parts; participants:

- took part in an end-of-study interview,
- edited exercises from Phase 1, and
- completed a modified version of the privacy classification survey that included questions specifically about social relations and was based partially on Ackerman’s survey in [1].

Sessions were approximately 60 minutes each. Data was collected in the form of materials completed by the participants, evaluator notes, and audio recordings.

Context-setting Location-Enhanced Applications

To help familiarize participants with location-enhanced technology, we described two hypothetical applications in Phase 1: single and standing request. In the *single request* application, people on a buddy list could make one-at-a-time requests for another user’s location, similar to existing location-enhanced applications like mMode’s Find People Nearby [8]. The *standing request* application used a less familiar model where a request could be sent to anyone on the buddy list for the requester to be notified whenever the user arrived at a certain location. For example, a user’s wife could request a notification every time he arrived at work. If he accepted the request, she would be notified every time he arrived at work, without another request being generated or him explicitly doing anything.

Several of the ESM questions explored these hypothetical applications. Questions asked participants how they would respond in their current situation given both single and standing requests for their location. Standing request questions asked participants to accept or reject the request. Single request questions allowed participants to send *something* or *nothing* about their location. When a participant decided to send *something*, he chose from the following location granularities:

- exact address (e.g., 1100 NE 45th St, Seattle, WA 98105),
- cross streets (e.g., 45th St. & 11th Ave),
- neighborhood name (e.g., University District),
- generic place name (e.g., home, work, park, etc.),
- ZIP code (e.g., 98105),
- city (e.g., Seattle),
- state (e.g., Washington), and
- country (e.g., United States).

If he did not want to disclose his location, he chose from the following responses:

- “System busy,”
- “I am busy,”
- “Request denied,” and
- a lie (which he could specify).

Selecting a response was often³ immediately followed by asking the participant why they made the choice they did, why they thought the requester might want to know their location, or what the ramifications would have been if something more or less detailed had been disclosed instead.

Participant Profiles

16 participants, eight male, from the Seattle area were recruited by a market research firm. Participants were aged

³ Certain questions were not asked in *every* questionnaire in an effort to reduce the time required of the participant.

24-64, left home daily, and regularly used their cell phones. 11 were employed full-time, one was training for a new job, three were part-time (two of whom were also students), and one was a homemaker. Participants with current or previous technical occupations were screened out. Their occupations varied, including Social Worker, Librarian, Financial Advisor, Teacher, Architect, Estate Planner, etc. 14 had a spouse or significant other; four had children.

The Westin/Harris Privacy Segmentation Model [18] was used in Phase 1 to determine to which basic privacy group each participant belonged: *fundamentalist*, *pragmatist*, or *unconcerned*. According to Privacy & American Business (P&AB), *fundamentalists* have “very high privacy concern” and are “passionate about what they [see] as business threats to their consumer privacy, and [favor] active government regulation of business and information practices.” *Pragmatists*, who are a “middle group with balanced privacy attitudes,” “ask what benefits they get as consumers in sharing their personal information to balance against risks to their privacy interests, and they usually favor a mixture of government and private solutions.” *Unconcerned* individuals have “little to no concern about consumer privacy issues.”

The breakdown of participants’ privacy classifications are shown in Table 1. The trends we saw in participants are slightly different than those reported by P&AB/Harris Interactive but similar to those found by Sheehan [22], with pragmatists being the largest group in our study, followed by unconcerned, then fundamentalists (P&AB/Harris reports more fundamentalists than unconcerned).

Table 1. Privacy classifications of the 16 study participants compared to P&AB’s reported numbers from 2003 and Sheehan’s online privacy study in 2002.

	P&AB '03	Sheehan '02	This Study
Fundamentalist	36%	3%	12%
Pragmatist	53%	81%	69%
Unconcerned	11%	16%	19%

Compensation and Participation Levels

Compensation was based on level of participation and was calculated based on the total number of ESM questionnaires completed out of 140 possible and days called into the voicemail diary out of 14 possible. Similar to the incentives used by Palen and Salzman in their voicemail diary study [20], compensation was structured to encourage maximum participation and varied from \$60 – \$250 USD.

All 16 participants fully completed Phases 1 and 3. Phase 2 participation varied, with an average response rate of 90.4%. 12 participants had a Phase 2 response rate of 95% or more. One participant was under 74%, completing only 42% of Phase 2 due to family emergencies. A total of 2,015 questionnaires were completed; each participant completed an average of 126 questionnaires. The overall high response rates imply that we were sampling participants in a variety of situations over the two weeks.

Caveats

Experience sampling reduces many biases associated with self-report, recall methodologies, because as Barrett points out [4], “[it] does not require retrieval or reconstruction of data from memory but rather involves access to and accurate reporting of information available to conscious awareness.” However, as with all self-report methodologies, experience sampling relies on the participants answering the questions honestly.

Additionally, participants were reacting to hypothetical requests⁴; *i.e.*, they did not have to deal with the ramifications of their responses. We believe that exploring social ramifications is an important next step and are deploying a working location-enhanced application [23] to do so. The results of this study were used to inform the design of that application.

KEY FINDINGS

In this section, we report on which factors affected whether and what participants would disclose to social relations. Overall, our results show that the most important factors were *who* was requesting (with subtleties like the participant’s current feelings toward the requester), *why* the requester wanted the participant’s location, and *what detail* would be most useful to the requester. Another interesting finding is that participants typically disclosed the most *useful detail* about their location (which is not necessarily the most detailed) or *did not disclose* their location at all.

Our study touched upon these and other aspects of location disclosure. Specifically:

- what the participants’ would disclose,
- the effect of the *relationship* of the requester to the participant,
- the effect of *where* the requester lived relative to the participant,
- the effect of the participant’s *location* when he received the request,
- the effect of the participant’s *activity* or *mood* when he received the request,
- the effect of the participant’s *privacy classification*,
- why participants rejected requests,
- what participants wanted to know about the *locations of others*, and
- participants’ *privacy and security* concerns.

The results we present are from the contextual and single-request-for-location questions, unless otherwise noted. When we discuss participants’ willingness to disclose, we are referring to their willingness to disclose *something*

⁴ Though requests were hypothetical, the qualitative responses suggest that requests received careful consideration.

about their actual location (*i.e.*, not responding with “I am busy,” “System busy,” “Request denied,” or a specific lie).

What Participants Would Disclose

Overall, participants were willing to disclose something about their location most of the time they received a request (which accounted for 77% of the 3,798 total requests⁵ they received). Of the time they were willing to disclose their location, they wanted to disclose something:

- *fairly specific* 77% of the time (exact address, generic place name—*e.g.*, home or work, or cross streets),
- *less specific* 19% of the time (neighborhood name, city, or ZIP Code), and
- *vague* only 5% of the time (state or country).

Our data suggest that blurring location⁶ to protect one’s privacy from social relations is not necessary, or at least is not something participants thought to use. Two types of results support this claim.

First, if participants were not willing to disclose their location at a level they thought would be *useful* to the requester, they chose to not disclose location at all. As one participant put it, “*If people want to know where I’m at, they want to know where I’m at.*”

Quantitatively, the fact that participants chose to respond with “less specific” or “vague” location information (*i.e.*, neighborhood, city, ZIP code, state, or country) only 24% of the time indicates that blurring was not commonly used. With regard to the 24% of less specific and vague disclosures, participants qualitatively told us that they often chose to disclose less specific information because they thought something less specific would be most useful to the requester and not because they were uncomfortable giving the requester more detailed information. For example, one participant went on a trip that spanned three states. While on that trip, she replied to requests with “state,” not because she wasn’t willing to share her exact address, but rather that she thought it would not have been “*useful*” to the requester. Other participants mentioned that requesters who lived in other states or countries would find city, state, or something less specific to be more useful than detailed information. One participant mentioned that more detail would have meant less to the “*out-of-state people.*”

Second, for some users, granularities like “city” could be quite descriptive. For one participant, <City A>⁷ meant that she was at her grandparents’ house, <City B> meant that

she was at work, <City C> meant that she was visiting her boyfriend, and so on. For other participants, this same principle applied when they were visiting clients, either around Seattle or the entire country.

Turning our attention to the 23% of the time participants were *not* willing to disclose their location to the requester, they responded with “I am busy,” “Request denied,” “System busy,” or a lie (in order of overall popularity). Participants chose to not disclose their location rather than merely blurring, which suggests that they were using the response to reinforce or communicate social boundaries. That is, they used the denial to send a message that the request was inappropriate. As one participant put it, *work people after work hours don’t get to know, except for one guy at work who is also a close friend.*

Relationship of Requester to Participant

Both the qualitative and quantitative data suggest that *who* the requester was had the strongest influence on participants’ willingness to disclose. When participants received a hypothetical request from their *significant others/spouses*, they were willing to disclose something for 93% of the 670 requests. Of the remaining 7% when participants did not want to disclose, they responded with “I am busy” 75% of the time; “I am busy” was also the most popular response in cases they did not want to disclose to social relations who were not significant others. Participants were also very willing to disclose location to their *friends* (85% of 902 requests) and *family* (83% of 1279 requests).

However, when requests came from *co-workers* and *managers*, participants were not as willing to disclose. They disclosed something to co-workers 53% of the 682 requests and managers only 34% of the 235 requests.

Other subtle factors regarding the requester affected decisions to disclose. First, the participant’s feelings toward the requester had an effect. After rejecting a request for her location, one participant wrote in a response to a follow-up question that she rejected the request because “[*the requester*] is being a butt.” Another mentioned in his Phase 3 interview that he and his mother got in an argument and he consequently rejected several of her requests.

Second, in the interviews, many participants mentioned that they needed to know *why* the requester wanted to know their location before responding to the request. In many cases, they felt they could reasonably guess, but in cases where they rejected location requests, they often said that the requester did not have a good reason to know.

Where Requester Lived Relative to Participant

When participants decided to disclose *something* about their location, *what* they disclosed varied based on where they lived relative to the requester. They disclosed exact address, generic place name (*e.g.*, home, work), or cross streets far more often to requesters who lived in the same city or state than to those who lived out-of-state (of the 2182 requests

⁵ Each questionnaire often contained more than one request. Results in Key Findings may not always add up to 3798, as not all questions were asked for every request and we have omitted some of the less interesting results for reasons of space.

⁶ *Blurring* location refers to disclosing something true but not specific, and is often suggested as a way to protect one’s privacy.

⁷ City names removed to protect the participant’s identity

where they disclosed *something* to same-city or state people, they disclosed something fairly specific 83% of the time and only 55% of the 643 *something* responses to out-of-state people). Table 2 shows the breakdown.

Table 2. What participants chose to disclose based on how near the requester lived to them.

In proximity to participant, requester lives ...	Address, Place name, or X-streets	Neighborhood, City, or ZIP Code	State or Country
in same city	86%	11%	3%
in same state, but not city	80%	19%	1%
out-of-state	55%	28%	17%

Responses when participants decided to disclose *nothing* about their location varied also. They were likely to disclose “I am busy” to requests from same-city relations (78% of the 272 rejections), whereas out-of-state requesters would receive “Request denied” for 54% of the 183 rejections (Table 3).

Table 3. How participants chose to respond when they rejected requests, based on how near the requester lived to them.

In proximity to participant, requester lives ...	I am busy	System busy	Request denied
in same city	78%	12%	10%
in same state, but not city	37%	13%	50%
out-of-state	41%	5%	54%

Location

Because of the high response rates and the two week sampling period, participants completed questionnaires in a variety of places. Figure 2 shows a breakdown of where participants reported they were when they responded to requests. Participants responded to requests about half the time at home, about a quarter of the time at work, and the rest of the time at various other places.

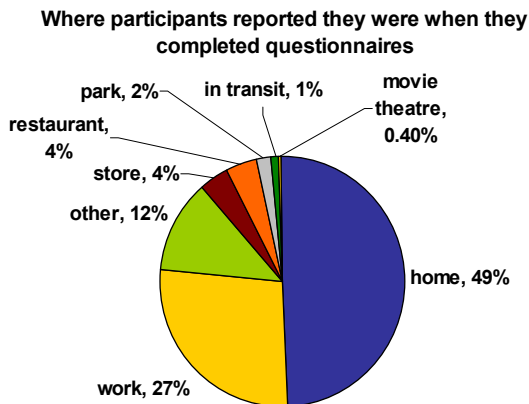


Figure 2. Participants responded to requests in several places, however, they were at home and work most often.

Examples of write-ins for the “other” response option were: “aquarium,” “concert,” “lake washington,” “babysitting for a friend,” “new york,” “my sister’s house,” “airport,” “ferry boat,” and “Canada.”

Based on the results from the voicemail diaries where participants reported if they went anywhere atypical for that day of the week, they went to an average of 13 “atypical” places over the 14 days of Phase 2. Those 13 atypical places were visited over an average of 9 days (*i.e.*, participants did not go anywhere atypical for 5 of the days). The range of atypical places visited was 4 – 23 and days they went to atypical places was 4 – 14⁸. These “atypical” places were occasionally work-related, but were more often visiting friends, stores/mall, the salon/barber, restaurants, movies, sporting events, general recreation, *etc.*

Where participants were when they received a request had an effect on whether and what they would disclose. Participants were often willing to disclose their location when they received a request at work (84% of the 1082 instances) and were fairly willing to disclose in “other” locations (76% of the 427 instances), at home (74% of the 1807 instances), and at stores (71% of the 136 instances).

Where participants were had an effect on whether they would disclose to co-workers and managers. When at work, participants were willing to disclose to co-workers and managers 80% (217 responses) and 69% (87 responses) of the time, respectively. With co-workers, participants were willing to disclose 55% of the time that they received a request at the grocery store (11 responses) and 47% of the time they were at home (362 responses). With managers, they were willing to disclose when they received a request at home only 24% of the time (117 responses). They were mostly unwilling to disclose to managers when they were at all other locations.

Activity & Mood

Factors other than requester relationship and participant location seemed to affect whether and what participants would disclose about their location. To explore these factors, we asked questions about the participant’s context at the time of the request, including activity and mood. We also explored these factors in the Phase 3 interviews.

ACTIVITY. What participants were doing when they received a request appeared to have some effect on whether they would disclose something about their location. For example, they were very willing to disclose something when they were doing household chores (96% of the 75 times all participants received a request while doing this activity). They were also fairly willing to disclose something when they were exercising (84% of 164 times) and talking on the phone (81% of 433 times). However,

⁸ This does not include an outlier who only went to two atypical places on one of the 14 days.

they were less willing to disclose when they were studying (63% of 40 times) or talking with a colleague in person (65% of 214 times).

MOOD. Mood also appeared to have some affect on responses. Overall, participants were most willing to disclose their location when they were “depressed” (disclosed 82% of 44 responses). They disclosed least often when “angry” (57% of 7 responses). Other moods included “happy” (77% of 804 responses), “calm, relaxed” (77% of 2481), “stressed” (72% of 308 responses), “sad” (64% of 25 responses) and “other” (84% of 129 responses).

Qualitatively, participants told us that their mood did impact their willingness to disclose their location. For example, one participant said, “*If I’m stressed or pissed off at the world, I don’t want anyone to know where I am.*”

Privacy Classification

The Privacy Segmentation Model used by P&AB/Harris Interactive has become a powerful and popular tool in the area of privacy evaluation. There is a danger, however, in generalizing its results beyond the business environment for which it was intended. Our study measured attitudes about location-oriented disclosures to members of one’s social network; this is quite different, for example, than giving one’s home address to a business. Thus it is not surprising that the participant’s privacy classifications as determined by the survey did not serve as a good predictor of their disclosure rates ($R=0.29$). On average, *unconcerned* participants disclosed something 58% of the time (with a range of 85%), *pragmatist* participants disclosed 88% of the time (range of 25%), and *fundamentalist* participants disclosed 70% of the time (range of 19%). Though *pragmatists* behaved as expected, *unconcerned* and *fundamentalists* did not. For example, the two participants who were least willing to disclose their location (12% and 41%) were both *unconcerned*, and *fundamentalists* usually chose to disclose their location.

To see if participants’ privacy classifications were correlated with their willingness to disclose location to a company, the ESM questionnaires included a question about how the participants would feel if their cell phone service provider had access to their current location within 100 yards⁹. Not surprisingly, *fundamentalists* indicated they did not like this 100% of the time and *pragmatists* did not like this 43% of the time. However, the *unconcerned* did not like it 77% of the time.

Rejecting Requests

As mentioned earlier, participants rejected 23% of the 3,798 requests for their location. Several participants were disturbed by requests that seemed inappropriate or out of character. These were often requests from the participants’

managers or co-workers during non-work hours, though some participants were disturbed during work hours as well. Comments included:

Regarding my boss, all she needs to know is that I’m getting my work done, not where I am.

During work, it was okay when a co-worker or boss wanted to know where I was, but it was weird when I was at the coffee shop.

However, one participant who normally rejected requests from his boss during non-work hours, chose to disclose his location to his boss’s requests on one Saturday during Phase 2. For just that weekend, a situation at work made the request appropriate.

Inappropriate requests were not limited to co-workers and managers. In some instances, it even seemed inappropriate when a friend made a request:

When I was socializing with my friends, other people’s requests seemed rude.

When my friend, who lives in Switzerland, wanted to know when I got to work – that was weird and out-of-character.

Several participants also mentioned that they would not want to use a single-request style application at many of the same times they do not use their cell phones. Most often, this was private time for the participant or time spent with those closest to them. Six participants used special names to describe these times, e.g., “<first name>’s time,” “me time,” “alone time,” a “me day,” and a “private day.” One participant talked about “date night,” which was a regularly scheduled event between her and her husband. At such times, participants did not want to be found by others.

Many participants mentioned that they did not want to disclose location to anyone when they were running errands, often with the exception of their significant others. One participant mentioned: *When I’m out and about, them knowing where I am is not beneficial and “would be a speed bump in my day.”* Other participants did not want the requester to add to their errands:

I wouldn’t want people to ask me to pick stuff up.

It would create a burden because someone else knows you’re there—you might have to do something for them too, which will take more time.

Occasionally, participants did not want their significant others to know where they were when they were doing something they were not “supposed” to do:

When I go to babyGap, I don’t want my husband to know (as he thought she spent too much money there).

...if I told my wife I was taking the dogs out for exercise and I really didn’t do it.

⁹ Phase II of Enhanced 911 [7] requires providers to be able to locate a mobile phone by approximately 100 yards.

What participants wanted to know about others

In half of the ESM questionnaires, participants were asked whose location they would want to request. Participants responded on 357 occasions and wanted to know the location of 907 others on those occasions, *i.e.*, they often wanted to know the location of more than one person (98% of these people were on their buddy list). Of the people on their buddy list, the average numbers of requests from participants per role were: 4.6 requests per family member (not significant other), 4.4 requests per friend, 3.5 requests per significant other, 3.4 requests per coworker, and 1.6 requests per manager. There was a statistically-significant, moderate correlation ($r = .488$, $p < .0001$) between the average number of requests for each group member's location and participants' willingness to disclose to members of that group (*i.e.*, participants were fairly likely to disclose to family members and they also were interested in knowing family members' locations fairly often).

After participants said that they would want the location of someone else, they were asked *what* they would want to know about the location. Participants wanted exact address (58% of the time), generic place name (13%), cross streets (12%), neighborhood name (11%), city (7%), and state & country (0.2%). The fact that participants requested neighborhood name, city, and state further indicates that these low detail levels can provide useful information.

Privacy & Security concerns

Nine of the participants mentioned privacy or security concerns regarding location-enhanced applications for social relations. For example, some participants mentioned concerns about their social relations knowing their location:

It would be "a little creepy" for people to always know where I am.

It's like being on a leash—like a cell phone, but I turn it off or don't answer it (this comment was specifically regarding disclosing to her manager and co-workers).

Others mentioned concerns about a third party or unintended individual spying on their information or getting hold of their actual device:

What if it gets lost and someone else comes across it or just looks at it—they can find out too much.

What if I lost it or somebody got hold of it?

The information would have to be secure. There would need to be restrictions such that only the people you want to have the information should get it. A thief could benefit from knowing where I am.

Other terms these participants used to describe concerns included "stalking," "being monitored," and "Big Brother."

DECISION PROCESS FOR DISCLOSING LOCATION TO SOCIAL RELATIONS

Based on the results of the ESM questionnaires and Phase 3 interviews, a pattern emerged in the way participants

described their decision process for location disclosure, which may be useful to designers of location-enhanced applications by helping them understand what is important to users. In interviews, we asked participants to share what contributed to their decisions of whether and what to disclose. As presented in previous sections, the most important factors were *who* was requesting, *why* that person was requesting, and *what* would be most useful to the person. After determining (or guessing) these, the participant would make a decision about whether or not they were willing to disclose this information to the requester. This decision process was qualitatively described by many participants in interviews, and is formalized here:

- 1) Who is making the request (and how do I feel about that person right now)?
- 2) Why does the requester need to know?
- 3) What would be most useful to the requester?
- 4) Am I willing to disclose that? (Because if I am not willing to disclose what is useful, I will not disclose.)

The quantitative feedback presented in the Key Findings section clearly shows that *who* the requester is plays a critical role in the participants' willingness to disclose location. The write-in responses from Phase 2 and interview data from Phase 3 highlight some subtleties of this point, such as the importance of *how the participant feels* about the requester at the time of the request.

In addition to the data presented in the Key Findings section, some Phase 3 interviews indicated that requests were rejected for lack of a good reason:

Would I want to talk with or be in contact with this person right now?

"My mother is nosy. It drives me crazy."

Why do they need it? Are they just bugging me or do they have a real reason?

Regarding steps 3 and 4 of the decision process, the participants' responses seem closely related to a phenomenon called *recipient design* [21] in conversation analysis where people carefully construct what they say "to match the needs and capabilities of recipients, taking account of such varied factors as shared background information and shared values" [9].

RELATED WORK

Several studies have explored the disclosure of private information (including, but not focusing on location information) and have made application design suggestions regarding the configuration of privacy preferences. Palen and Dourish [19] argued that our lives are not predictable, and concluded that privacy management is a dynamic response to circumstance rather than a static enforcement of rules. Similarly, Lederer *et al.* [15] warned that designs should not require excessive configuration to create and

maintain privacy, since configurations are de-situated from the contexts to which they apply. Together, these studies argue that *a priori* configuration of applications that disclose private information will usually not work.

However, *a priori* configuration of privacy management has the benefit of enabling systems to act on a user's behalf in a way that he specifies without having to interrupt him with every request. Several projects provide evidence that this may be possible. Olson *et al.* [17] studied the disclosure of private information (*e.g.*, age, phone number, credit card number, email content, income, health, current location, *etc.*) to social relations and the public. In a survey, participants were asked about their willingness to disclose this information to others by *role* (spouse, parent, manager, people who work for me, salesperson, *etc.*). Their results showed that people treat clusters of social relations similarly. The clusters they identified were the public, high level corporate types, coworkers, manager, family, and spouse. They concluded that users of applications that disclose private information may be able to set preferences for sharing based on clusters of requesters. This would reduce configuration overhead, as many requesters can be represented by a small number of clusters.

In another project, Hull *et al.* [12] presented the Houdini rule engine, and argued that rule configuration will enable privacy-conscious user data sharing. Finally, Begole *et al.* [5] identified patterns in people's daily activities in a study of office workers. They showed that there is significant routine in daily office life, which implies that a privacy managing system may be able to act for users in certain predictable office situations.

In our study, we preceded the ESM phase by asking participants to predict the factors that would affect their decisions to disclose their location and formulate disclosure preferences for individuals and/or groups of social relations. Then, we formulated questions to gather information about what factors actually affected their decisions to disclose. Our qualitative results indicate that participants saw pre-formulated preferences as a useful starting point, but they would like to be able to easily change the preferences and to turn off the application, or at least the automatic disclosures, when desired. Our quantitative results do not definitively show that *a priori* preference configurations are or are not useful in the case of disclosure to social relations.

Other studies have explored the factors that people use to make decisions regarding privacy disclosure. Adams [2] conducted a study of privacy concerns in an audio/video-captured environment. Results showed that user perception of privacy was shaped by the perceived identity of the information *receiver*, the perceived *usage* of the information, the subjective *sensitivity* of the disclosed information, and the *context* in which the information was disclosed. Lederer *et al.* [16] built on this work, finding in a survey study that *who* is inquiring is more important than the user's *context* in deciding what to disclose about private

information (*i.e.*, identity, email, occupations, interests, current activity, and location).

Barkhuus and Dey [3] investigated users' thoughts about usefulness and concern with location-tracking and position-aware services. Their study included 16 mobile phone users aged 19-35 who answered pre-specified questions in a journal over 5 days. A subset of the participants were interviewed to elaborate on their journal entries. Their results revealed that though the perceived usefulness of both types of services was about the same, the location-tracking services generated more concern for privacy.

In addition to exploring privacy disclosure, some have incorporated Westin's privacy classifications into studies. For example, Ackerman [1] conducted a survey of online users to explore their e-commerce privacy concerns. Sheehan [22] conducted an email survey with 889 U.S. Internet users that used a variety of online communication-related scenarios to assess their privacy concerns. Based on her results, Sheehan created a new grouping of privacy classification for Internet users to highlight some of the obvious differences in the pragmatist group. Her categorizations of Internet users' privacy classifications are *unconcerned*, *circumspect*, *wary*, and *alarmed*.

Our results regarding the most important factors in location disclosure to social relations complement the findings of Adams and Lederer. However, we gathered quantitative results *in situ* that showed certain factors are more important than others. *Who* was requesting and *why* they wanted to know were most important; our qualitative results suggest that "how I feel" about the requester at the time of the request is also an important factor. User *location* and *activity* (Adams' *context*) was found to be a factor of lesser importance, as supported by Lederer *et al.* [16].

CONCLUSION & FUTURE WORK

In this paper, we presented the key findings of our initial explorations into users' disclosure of location to social relations. These findings came from a 16-participant study that involved a variety of techniques—both in lab and *in situ*—including questionnaires, the Westin/Harris Privacy Segmentation Model, exercises, two weeks of Experience Sampling, a nightly voicemail diary study, and interviews. Our most notable findings are that:

- participants want to disclose what they think would be useful to the requester or deny the request, and
- participants' privacy classification, as determined by the Westin/Harris Privacy Segmentation Model, was not a good predictor of how they would respond to requests for their location from social relations.

From our results, we reflected on the process participants went through to determine whether and what to disclose about their location to requests from social relations: *i.e.*, *who* is requesting, *why* do they need to know, *what* would be most useful to them, and *am I willing* to share that?

Much work remains. Our next step is to deploy a working location-enhanced application to explore how introducing social ramifications affects disclosures to social relations. This should also help us learn about how often requesters typically want to know a user's location and what the balance should be between a system that the user controls and therefore interrupts him versus one that relies on *a priori* preference configuration. Also of interest are the longevity of the user's location information and who should have access to it. We would like to further investigate the use of the Westin/Harris Privacy Segmentation Model as it relates to user's location disclosure to institutions/services, their employers, other organizations, and the government.

ACKNOWLEDGMENTS

We would like to thank P&AB for allowing us to reprint the privacy classification definitions and their percentages from 2003, Jennifer Rode for her help with the study administration, and Mark Ackerman for sharing his privacy survey with us. We would also like to thank Scott Mainwaring, Ken Anderson, Christine Riley, James Landay, David McDonald, Jason Hong, Jennifer Mankoff, Paul Dourish, Barry Brown, and Tanzeem Choudhury for their advice.

REFERENCES

1. Ackerman, M.S., *et al.* "Privacy in E-Commerce: Exploring User Scenarios and Privacy Preferences," In *Proc. of the ACM Conf on Electronic Commerce: EC '99*, pp. 1-8.
2. Adams, A. "Multimedia information changes the whole privacy ballgame," In *Proc. of Computers, Freedom & Privacy '00*, 2000, pp. 25-32.
3. Barkhuus, L. and Dey, A., "Location-Based Services for Mobile Telephony: a study of users' privacy concerns," *Proc. of Interact '03*, Zurich, 2003, pp.709-712.
4. Barrett, L.F., Barrett, D.J., "An Introduction to Computerized Experience Sampling in Psychology," *Social Science Computer Review*, Vol. 19, No. 2, (Summer 2001), pp.175-85.
5. Begole J., *et al.* "Work rhythms: Analyzing visualizations of awareness histories of distributed groups", In *Proc. of CSCW '02*, pp. 334-343.
6. Consolvo, S. and Walker, M., "Using the Experience Sampling Method to Evaluate UbiComp Applications," *IEEE Pervasive Computing Mobile and Ubiquitous Systems*, Vol. 2, No. 2, Apr-Jun 2003, pp. 24-31.
7. "Enhanced 911," *911 Services* section, Federal Communications Commission: <http://www.fcc.gov/911/enhanced/> (verified Jan 4, 2005).
8. "Find People Nearby," *mMode* section, Cingular/AT&T Wireless website: <http://www.attwireless.com/personal/features/organization/findfriends.jhtml> (verified Jan 4, 2005).
9. Goguen, J., "Are Agents an Answer or a Question?" *Proc. of the JSAI-Synsophy International Workshop on Social Intelligence Design*, 2001.
10. Hong, J.I., Landay, J.A., "Support for Location: An Architecture for Privacy-Sensitive Ubiquitous Computing," In *Proc. of Mobisys '04*, Boston, Jun 2004, pp.177-89.
11. Hong, J.I., *et al.* "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems." In *Proc. of DIS '04*, Cambridge, MA, pp. 91-100.
12. Hull, R., *et al.* "Enabling Context-Aware and Privacy-Conscious User Data Sharing," *Proc. of the IEEE International Conference on Mobile Data Management: MDM '04*, pp. 187-98.
13. iESP software website: <http://seattleweb.intel-research.net/projects/esm/iESP.html> (verified Jan 6, 2005).
14. Kochen, Manfred, Ed. *The Small World*. Ablex, Norwood, NJ, 1989.
15. Lederer, S., Hong, J.I., Dey, A.K., Landay, J.A., "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," *Personal and Ubiquitous Computing*, Vol. 8, Number 6, Nov 2004, pp.440-54.
16. Lederer, S., Mankoff, J., Dey, A.K.. "Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing." In *Extended Abstracts of CHI 2003*, Apr 2003, pp.724-5.
17. Olson, J.S., *et al.* "Preferences for Privacy Sharing: Results & Directions," *CREW Technical Report*. 2004.
18. P&AB, "Consumer Privacy Attitudes: A Major Shift Since 2000 and Why," *Privacy & American Business Newsletter*, Vol. 10, Number 6, Sep 2003.
19. Palen, L. and Dourish, P., "Unpacking "privacy" for a networked world," *Proc. of CHI '03*, pp. 129-136.
20. Palen, L. and Salzman, M., "Voice-mail diary studies for naturalistic data capture under mobile conditions," *Proc. of CSCW '02*, pp. 87-95.
21. Sacks, H., *et al.* (eds), *Lectures on Conversation*, Blackwell Publishers Jan 1995.
22. Sheehan, K., "Toward a Typology of Internet Users and Online Privacy Concerns," *The Information Society*, Vol. 18, No. 1, 2002, pp.21-32.
23. Smith, I., Consolvo, S., Hightower, J., Hughes, J., Iachello, G., LaMarca, A., Scott, J., Sohn, T., Abowd, G., "Social Disclosure of Place: From Location Technology to Communication Practice," *Proc of the 3rd Int'l Conf on Pervasive Computing: Pervasive '05*, Munich, Germany (May 2005 - to appear).