Understanding the Implications of Offering More Disclosure Choices for Location Sharing

Karen P. Tang
Donald Bren School of Information & Computer Sciences
University of California, Irvine
kptang@ics.uci.edu

Jason I. Hong, Daniel P. Siewiorek
Human-Computer Interaction Institute
Carnegie Mellon University
{jasonh, dps}@cs.cmu.edu

ABSTRACT
We compared two privacy configuration styles for specifying rules for social sharing one's past locations. Our findings suggest that location-sharing applications which support varying levels of location granularities are associated with sharing rules that are less convoluted, are less likely to be negatively phrased, and can lead to more open sharing. It also results in higher perceived comfort scores, which could be indicative of a false sense of control.

Author Keywords
Privacy, rules, configuration, location sharing.

ACM Classification Keywords
H.3.5. Online Information Services: Data Sharing.

INTRODUCTION
Advances in location sensing and mobile technology have made it easy for people to share their location with others. Many location-sharing applications (LSAs) frame these disclosures using social motivations, stating that awareness of others' current location can encourage more social serendipity and better social grounding [8]. However, location sharing also exposes end-users to potential privacy risks. Consider Foursquare and Facebook Places, which lets users browse historical feeds of their friends' locations. With these LSAs, more location information is being shared within one's network, as these feeds have implicitly turned what was once *current* location sharing into a now much more persistent and continuous sharing of *past* locations.

Sharing historical data, however, is a double-edged sword. On one hand, sharing more data provides better awareness of a person's whereabouts and activities, which can be helpful for increasing social capital between weak ties [7]. On the other hand, sharing data streams often makes it easier to aggregate information and trends. For example, by sharing past locations, one could infer potentially personal information like travel routines (e.g., when someone arrives home, what routes they take when going home) or favorite activities (e.g., which restaurants someone frequents). In light of these privacy risks, it is important to design privacy controls specifically for sharing *past* locations.

CHI'12, May 5–10, 2012, Austin, Texas, USA.

One repeated finding in the privacy literature is that LSAs should support varying levels of granularity [6, 8, 9, 11, 12, 15]. Providing both precise and vague descriptions of location allows for plausible deniability [9], a necessary social phenomenon that provides better impression management [15]. Other work has revealed that there are additional factors which can be helpful in configuring sharing preferences, including mood [6], time [13], and geographic references [13]. Nearly all of these studies have been conducted on scenarios for sharing *current* locations.

In our work, we investigate whether these same factors are useful for sharing *past* locations. More importantly, we also investigate the implications of designing privacy configurations that support large sets of privacy filters. Based on 30 interviews, our results suggest that configurations that support varying location granularities can lead to sharing rules that are less complex, more open, and are selections that users are more comfortable with. These results have important implications for future LSAs that are weighing the benefits of having flexible privacy controls for specifying sharing preferences.

RELATED WORK
For LSAs, it is common to find privacy controls where users must specify with whom to share their locations. Many systems use a buddy list, where locations are only shared with people on that list [3, 14]. Other systems use group-based controls [8, 12], incorporate different location granularities [8, 9, 12], or allow users to specify when disclosures should occur [12, 13]. Some LSAs have used mood-based privacy preferences as well [6]. Each of these privacy filters has been used in the context of sharing *current* locations. In our work, we examine whether these filters are also useful for sharing *past* locations.

To do this, we examine two different privacy configuration styles (Table 1). The baseline configuration style uses an all-or-nothing approach that is commonly seen in current LSAs, where users either share no location information or a specific geographic description (an address or intersection). The experimental configuration style allows users to share varying granularities of location information that are less descriptive than an address or intersection. In both configurations, users can use privacy filters to restrict the conditions in which their location is shared with others. These filters are based on past work and include limiting sharing by mood, time, and receiver type.

Our work provides an initial look at the implications for designing privacy controls that support *multiple* privacy filters. Past work in economics have shown that providing a large choice set can have both positive and negative effects. On one hand, having more choices offers a better match between one's preferences and allows for more flexibility in one's decision making [10]. However, deciding amongst several choices can also lead to an increased cognitive load for users, a greater sense of confusion, and a less satisfying decision [5]. In our work, we look at how additional disclosure options influences location privacy preferences.

In summary, our study compares two configuration styles for specifying privacy preferences for location sharing. We focus on two research questions. First, we explore how different configuration styles affect users' sharing preferences. Second, we assess users' perceived comfort levels with their specified set of sharing preferences and understand the implications for how end-user perception might impact the design of future LSA privacy controls.

STUDY DESIGN

We recruited 30 participants, ages 20-54 years ($\bar{x}$=28.1, sd=7.3), from a local university; 18 participants were male. 10 participants were undergraduates, 11 were graduate students, and nine were administrative staff. Of the 21 students, thirteen had non-technical backgrounds.

Recruitment for the study was advertised as a usability evaluation of a university-wide experimental LSA for mobile phones called Social Beacon. These evaluations were conducted as hour-long interviews. Each interview began with an online tutorial explaining Social Beacon's location-sharing features and was based on seven scenarios describing why one might choose to share his location with others. These scenarios revolved around three themes: 1) to increase awareness about others (e.g., find out where friends went last night), 2) to meet new friends (e.g., find others who frequent the same places), and 3) to get recommendations (e.g., based on past visits, someone suggests a new restaurant). The tutorial also explained that, by default, Social Beacon would continuously update participants' locations and automatically share this data with others within the university. In particular, whenever location information was shared, Social Beacon would disclose one week's worth of *past* locations, in addition to the user's *current* location. To change this behavior, users could configure their own sharing settings.

We then presented two kinds of privacy configurations for specifying sharing preferences and counter-balanced them for ordering effects. In each configuration, participants defined a sharing rule using the privacy filters and disclosure granularities available for that particular configuration. To ensure that participants openly expressed their rules in as flexible a manner as possible, the rule specifications were done as pen-and-paper exercises. Participants were instructed that the researchers would later add their written rules into the system after installing the application. In reality, Social Beacon was a hypothetical LSA used to ground considerations of privacy concerns for location sharing. To maintain the system's realism, we only recruited participants who owned smartphones, as this LSA would have been deployed on such a platform. At the end of the study, we disclosed our experimental manipulation.

	Baseline	**Experimental**
Location Granularity	*Nothing* or *Specific geographic* (address)	*Nothing*, *Specific geographic* (address), *General geographic* (city or neighborhood), *Specific semantic* (business names, like Starbucks or personal labels, like home), or *General semantic* (type of place, like coffee shop)
Privacy Filters	*Time of Day* (5-8pm, evenings), *Day of Week* (weekends), *Frequency of Visits* (after 2 visits), *Current Transportation* (driving, walking), *Current Mood* (positive/neutral/negative)	

Table 1. The privacy configurations differed in the location granularities offered, but offered the same privacy filters. Examples of granularities & filters provided in parentheses.

Privacy Configuration Exercises

In each privacy configuration, participants defined rules for how Social Beacon should share their locations. Each rule was required to have three parts: 1) who they want to share their location with, 2) how the location should be described (i.e., what level of location granularity should be shared), and 3) under what conditions should the location be shared. When specifying the "who" portion of the rule, each participant referenced the same set of 8 relationship types: strangers, classmates/coworkers, acquaintances, casual friends, close friends, spouse/significant other, bosses/ professors, and family members. These relationship types were based on past work involving location sharing [2, 6].

The two privacy configurations differ only in the types of location descriptions that can be shared with others. The baseline configuration is modeled after the "all-or-nothing" approach that many existing LSAs use for location sharing. In this configuration, users choose between sharing no geographical information or a precise geographical description (as depicted by a pin on a map, like an address). In the experimental configuration, users can share nothing or choose from four location abstractions, borrowed from past work [11, 15]. These abstractions can be semantic or geographic references that are general or specific (Table 1).

In both conditions, participants can add privacy filters to specify the conditions in which they would like to share their locations. Participants add these filters by using subordinate conjunctions (e.g., "except", "only if") and can reference 5 variables (Table 1): time of day, day of week, frequency of visits, their current transportation mode, and their current mood (positive, negative, or neutral).

Limitations of Study Design

Our study uses paper-based privacy configuration exercises and a hypothetical LSA. We used several techniques to

ensure that Social Beacon's status was not apparent to participants. In fact, all of our participants were surprised to learn that no software would actually be installed. It is possible that the privacy configurations measured people's *perceived* preferences rather than their actual preferences, similar to past ecommerce studies [1]. To alleviate this concern, we followed a think-aloud protocol to encourage participants to reflect and consider their privacy concerns, similar to what was done in [6]. Interview responses seemed to confirm that participants were thoughtful when expressing their sharing preference for location sharing.

KEY FINDINGS

Our participants created 121 and 148 privacy rules in the baseline and experimental configurations, respectively.

Q1a: Expressions of Sharing Rules: Who, What, When

Table 2 (top) shows how many participants shared their locations for each relationship type in both conditions. As expected, in the baseline configuration, participants were more willing to share with spouses and family, and least willing to share with bosses and strangers. This finding echoes past results that say people are more comfortable sharing with their close ties than with their weak ties [15].

Since Social Beacon was advertised as a university-wide LSA, there is an implicit social network for location sharing. The link between LSAs and SNSs is important. Past work has shown that SNSs typically have more weak ties (casual friends) than strong ties (close friends) [7]. This property has important implications for location sharing. Rows D-G in Table 2 make up the types of weak-tie relationships that are typically found in SNSs (while row F is also a weak tie, few users include a significant number of strangers in their SNSs). The baseline condition shows very few participants chose to share past locations for these groups ($\bar{x}$=1.0/30). In the experimental configuration, many more shared some level of their past location information with these groups ($\bar{x}$=17.25/30). These results suggest that additional location granularities can lead to significantly different sharing outcomes (McNemar's $\chi^2(1)=8.40$, $p<0.003$) and may encourage participants to share past locations when they would not have done so otherwise. When considering all relationship types, participants were more likely to hide past locations in the baseline condition. This result is similar to prior work [11], but show that they extend to sharing of past (and not just current) locations.

Table 2 (bottom) shows how often each privacy filter appeared in participants' sharing rules. For example, the most popular filters referenced time and day variables. 41 rules in the baseline configuration referenced a time or day (33.9%). In the experimental configuration, 26 rules contained time- or day-related privacy filters (17.6%). As these make up a non-trivial percentage of all the user-defined sharing rules, this suggests that LSAs should consider including temporal filters in their privacy controls.

An important finding we observed is that the experimental configuration resulted in less complex sharing rules (i.e., having fewer sharing conditions). We observed that the experimental rules contained fewer subjective conjunctions (McNemar's $\chi^2(1)=5.38$, $p<0.02$) and referenced fewer privacy variables (McNemar's $\chi^2(1)=75.2$, $p<0.0001$). Thus, participants were more likely to share rules like "always share my general geographic location" (no subjective conjunction or privacy filters) vs. "only share my location if I'm in a good mood and it's a weekend" (multiple privacy filters, expressed with the subjective conjunction "only if"). Having less complex rules is an important outcome, as simpler rules tend to require less cognitive load for when users need to re-examine their privacy preferences. Moreover, as computer-mediated communication becomes more context-aware, other types of data, beyond location, will also be shared. Thus, having simpler sharing rules for one type will be a more scalable privacy solution for when context-aware apps support other kinds of sharing. We do note though that, by adding location granularities, we are also inherently adding a level of complexity to the design of an LSA's privacy UI. Thus, while the resulting rule set is structurally simpler, further work is needed to address how to incorporate the privacy filters and location granularities into a UI so that it does not visually overwhelm users.

		Baseline Configuration		Experimental Configuration				
		No Location	Specific Geographic	No Location	General Semantic	Specific Semantic	General Geographic	Specific Geographic
A	Spouse/Sig. Other	1	29	0	19	3	3	16
B	Family	10	20	5	6	0	20	5
C	Close Friends	20	10	1	4	16	9	9
D	Casual Friends	29	1	12	5	0	16	0
E	Acquaintances	29	1	16	2	0	13	0
F	Classmates/Coworkers	28	2	9	4	0	21	0
G	Boss/Professors	30	0	0	0	0	16	0
H	Strangers	30	0	0	0	0	11	0

	Time	Day	Frequency of Visits	Transportation	Mood	Time+Day	Time+Day+Mood	No Filters
Baseline	5	11	0	5	9	8	17	66
Experimental	8	11	2	5	8	4	3	107

Table 2. (top) # of participants (out of 30) that preferred a certain location granularity for each relationship. Numbers may be >30 in the experimental condition since participants can share ≥1 location granularities. (bottom) # of rules containing the specified filters to limit location sharing ("only share if..."). A rule can contain multiple filters or no filters.

Q1b: Negative vs. Positive Phrasing of Sharing Rules

23.6% of the baseline rules had negative sharing language (e.g., "do *not* share my location if I'm in a bad mood" vs. "do share my location if I'm in a good or neutral mood"). In contrast, this occurred in significantly fewer experimental rules (10.8%; McNemar's $\chi^2(1)=52.1$, $p<0.0001$). In past work, negative rules were only examined in terms of blacklists, where users specified who should not receive their data. To our knowledge, this is the first study to examine how negative, exclusionary language in the context of other privacy variables. In particular, our findings suggest that LSAs should build privacy UIs to support negative phrasing, as it may be a better match to how participants naturally express their privacy concerns. Most existing LSAs rely almost exclusively on positive phrasing (e.g., "only share my location in X condition").

Q2: Perceived Comfort of User-Defined Rule Sets

Using a 5-point Likert scale, participants reported higher comfort scores ($\bar{x}_e=3.9$, $sd_e=0.68$; $\bar{x}_b=3.2$, $sd_b=0.71$) in the experimental configuration (Mann-Whitney=240, $p<0.001$). On one hand, this result is promising because, as previously indicated, the experimental configuration led users to share their location information in more situations and to more relationship types. Thus, it is encouraging to see that more sharing did not decrease users' perceived comfort level.

DISCUSSION

In our work, we present a comparative study using location granularity as an independent variable to determine its impact on end-user privacy preferences for location sharing. Our study also investigates these issues in the context of a group-based approach that also supports various privacy filters. This experimental design is distinct from prior work in that prior studies have examined privacy rules along one, but not all, of these dimensions. For example, IMBuddy [7] looked at privacy rules that supported different location granularities, but without the use of privacy filters. Work by Benisch et al. considered some privacy filters but did not vary location granularity and they used optimization-based equations to calculate users' sharing preferences [4]. This is distinct from our user-centric approach that references a user's natural expression of their sharing preferences through several privacy configuration exercises.

Despite these differences, several past studies have reported perceived comfort scores, though this is all done in the context of sharing only *current* locations. For example, past work has found that user were more comfortable sharing current locations with varying location granularity [6, 9] and when using time-related privacy filters (vs. no filters) [4]. Our work extends these results in two ways. First, we show that these user preferences persist when sharing *past* locations. Second, we show that, even when presented with several types of privacy filters, users still prefer having additional location granularities. In other words, users did not seem to mind the additional complexity of adding more disclosure options for sharing past locations.

CONCLUSION AND FUTURE WORK

In conclusion, our results show that privacy configurations that support varying location granularities can significantly change how privacy rules are defined and under which conditions locations are shared. In particular, we provide empirical evidence that including more abstract location descriptions can lead to more open location sharing, less complex rules, and fewer negatively phrased rules. Users were also more comfortable with privacy configurations that offered more granularities. In future work, we will implement our privacy configurations in an actual LSA, so that we can evaluate whether including additional location granularities enables LSAs to better match users' perceived preferences, as well as their real-world privacy preferences.

REFERENCES

1. Ackerman, M.S., Cranor, L.F. and Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In E-Commerce '99, 1-8.
2. Anthony, D., Kotz, D. and Henderson, T. (2007). Privacy in Location-Aware Computing Environments. IEEE Pervasive Computing, 6 (4), 64-72.
3. Barkhuus, L., Brown, B., Bell, M., et al. (2008). From Awareness to Repartee: Sharing Location within Social Groups. In CHI '08, 497-506.
4. Benisch, M., Kelley, P.G., Sadeh, N., et al. (2011). Capturing Location Privacy Preferences: Quantifying Accuracy and User Burden Tradeoffs. PUC, to appear.
5. Chernev, A. (2003). When More Is Less and Less Is More: The Role of Ideal Point Availability and Assortment in Consumer Choice. J of Consumer Research, 30 (2), 170-183.
6. Consolvo, S., Smith, I., Matthews, T., et al. (2005). Location Disclosure to Social Relations: Why, When, & What People Want to Share. In CHI '05, 82-90.
7. Ellison, N.B., Steinfield, C. and Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. Journal of Computer Mediated Communication, 12 (4), article 1.
8. Hsieh, G., Tang, K.P., Low, W.Y., et al. Field Deployment of Imbuddy: A Study of Privacy Control and Feedback Mechanisms for Contextual Im. In Ubicomp '07, 91-108.
9. Iachello, G., Smith, I., Consolvo, S., et al. Control, Deception, & Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. Ubicomp '05, 213-231.
10. Lancaster, K. (1990). The Economics of Product Variety: A Survey. Marketing Science, 9 (3), 189-206.
11. Lin, J., Xiang, G., Hong, J.I., et al. Modeling People's Place Naming Preferences in Location Sharing. Ubicomp '10, 75-84.
12. Patil, S. and Lai, J. (2005). Who Gets to Know What When: Configuring Privacy Preferences in an Awareness Application. In CHI '05, 101-110.
13. Sadeh, N., Hong, J.I., Cranor, L., et al. (2008). Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. PUC, 13 (6), 401-412.
14. Tang, J.C., Yankelovich, N., Begole, J., et al. (2001). Connexus to Awarenex: Extending Awareness to Mobile Users. In CHI '01, 221-228.
15. Tang, K.P., Lin, J., Hong, J.I., et al. (2010). Rethinking Location Sharing: Exploring the Implications of Social-Driven Vs. Purpose-Driven Location Sharing. In Ubicomp '10, 85-94.