My Privacy Policy: Exploring End-user Specification of Free-form Location Access Rules

Sameer Patil[1], Yann Le Gall[2], Adam J. Lee[2], and Apu Kapadia[1]
{patil, kapadia}@indiana.edu, {ylegall, adamlee}@cs.pitt.edu

[1] School of Informatics and Computing, Indiana University, Bloomington, IN 47408
[2] Department of Computer Science, University of Pittsburgh, Pittsburgh, PA 15260

Abstract. The increasing inclusion of location and other contextual information in social media applications requires users to be more aware of what their location disclosures reveal. As such, it is important to consider whether existing access-control mechanisms for managing location sharing meet the needs of today's users. We report on a questionnaire ($N = 103$) in which respondents were asked to specify location access control rules using free-form everyday language. Respondents also rated and ranked the importance of a variety of contextual factors that could influence their decisions for allowing or disallowing access to their location. Our findings validate some prior results (e.g., the recipient was the most highly rated and ranked factor and appeared most often in free-form rules) while challenging others (e.g., time-based constraints were deemed relatively less important, despite being features of multiple location-sharing services). We also identified several themes in the free-form rules (e.g., special rules for emergency situations). Our findings can inform the design of tools to empower end users to articulate and capture their access-control preferences more effectively.

1 Introduction

The popularity of online social networks has resulted in an unprecedented amount of sharing of personal information. Furthermore, the extensive use of mobile devices enables and encourages broadcasting *contextual* information wherever one happens to be. For instance, location-sharing systems, such as Facebook Places, Google+, and Foursquare, allow users to share their current location with friends. Recent technologies like Cenceme [10] can determine the current activity (e.g., "running" or "dancing") from a smartphone's onboard sensors. With the growing availability of ways to share personal contextual information, personal privacy management has become increasingly important and also more difficult.

Several studies have examined location-sharing preferences of end users. However, most prior work has focused on user specification of simple rules for controlling location disclosure. For example, many location-sharing systems—including commercial systems mentioned above as well as those in the research literature [4, 10, 13, 17, 18]—allow users to set up access-control rules based only upon *who* is accessing their location, or *when* this information is being accessed. Given the increasing adoption of location sharing, whether these types of simple rules are sufficient for capturing the access-control preferences of today's social media users is an open question.

Toward this end, we set out to understand (i) which contextual factors are deemed important by users when developing rules for controlling access to their location, and (ii) how users express access-control rules in everyday language. Understanding the importance of various contextual factors in location-sharing decisions can help guide the design (in terms of both features and user interface) of frameworks for authoring structured personal policies for location sharing. Further, understanding how users express location access-control rules using everyday language can provide insight into how tools for rule specification should be realized: e.g., imprecise free-form rules support the case for designing more structured editors to capture user intent, while high precision statements motivate natural language (i.e., 'Siri-like') interfaces.

We report on an online questionnaire conducted to explore these issues. The questionnaire asked respondents about preferences for access to their location. In particular, respondents rated and ranked the importance of a variety of contextual factors (such as the recipient of location information, the time of day, and the disclosure specificity) in making location-sharing decisions. We also collected free-form natural-language statements in which respondents described how they wish to manage access to location. Some interesting findings from our data include the following:

- The recipient of the location information was the most highly rated and ranked factor. This finding echoes prior research. However, the time and the day of location disclosure exhibited the lowest ratings and rankings, which was unexpected.
- Respondents found it difficult to express complex or even complete location-sharing rules in everyday language. Further, the factors mentioned in these statements often did not reflect the relationships observed in numeric ratings and rankings of the same factors.
- Participants did not seem to consider social nuance and technical limitations of their policy statements, such as the social implications of denying access to someone or the inability to revoke location disclosures that had already taken place.
- The rules included several recurring themes and factors. For example, many respondents desired means to facilitate location access during emergency situations and to exercise manual controls, such as the ability to apply temporary blocks on location tracking.

These findings can inform how location-sharing systems could be made more privacy-sensitive. For instance, in addition to recipient-based access control, location-sharing systems often offer settings based on temporal considerations. Therefore, it is notable that *time* and *day* were rated and ranked lower than other contextual factors. This result suggests that the usability of privacy controls in current location-sharing systems might not be well aligned with user preferences; systems rarely provide the ability to specify privacy preferences for other factors indicated as being important, e.g., frequency of access or one's current location. Also, the low expressivity of the free-form access control statements suggests several potential interpretations and implications. It might be the case that people are generally not able to articulate their privacy preferences. If so, designers can aid the creation of policy statements using structured rule specification interfaces. On the other hand, users may not be adequately motivated to specify details.

2 Related Work

Prior work on access control in location-sharing applications falls into two broad categories: factors influencing sharing and idioms for privacy-policy expression. We briefly survey key prior work and indicate differences with our study.

Factors influencing sharing: Lederer et al. [8] conducted a study to determine the relative importance of two factors: the recipient of location information and the user's current situation. They found that the recipient had a larger influence on privacy preferences. Consolvo et al. [4] conducted an experience-sampling study in which 16 participants responded to simulated location requests. They found that location disclosure was influenced by the recipient of location information, the reason for the request, and the level of detail revealed. Tsai et al. [18] discuss field deployment of *Locyoution*, a location-sharing application integrated with Facebook. They discovered that user comfort with sharing increased when given feedback regarding who accessed their location. However, Locyoution users were limited to time-based location-disclosure rules. Toch et al. [16] engaged in a four-week field study of the *Locaccino* system using a statistical approach to examine the relationship between locations and corresponding privacy preferences. Their data showed that users tended to feel more comfortable sharing in public places visited by many people. Wagner et al. [19] further carried out a 16-participant study in which subjects drawn from a university population were trained in the use of the Locaccino system and questioned about sharing preferences. They found that highly-granular location information was shared only when there was a perceived need and that subjects preferred not to broadcast location. Benisch et al. [1] collected location data from the phones of 27 people for 3 weeks. They observed that participants were more comfortable with location- and time-based policies to share with friends, family, or advertisers. A recent study by Schlegel et al. [15] found that individual perceptions of privacy loss varied greatly according to who was accessing the individual's location and how often this location was accessed.

Idioms for policy expression: Brodie et al. [3] examined the utility of natural-language policy authoring in the SPARCLE policy workbench. Employees from various organizations were tasked with crafting organizational policies, which were converted to XACML using shallow parsing. This work demonstrated the viability and utility of allowing people to specify certain types of policies using free text. Sadeh et al. [14] studied privacy concerns in the context of *PeopleFinder*, a location-sharing system for laptops and mobile devices. Lab experiments and field studies showed that PeopleFinder users were often dissatisfied with the location disclosures that their rules permitted, even after revising initial rules. Users were, however, consistent in their (dis)satisfaction feedback regarding location disclosures; the authors propose using this feedback to bootstrap machine learning techniques to generate and refine disclosure rules. Kapadia et al. [5] studied the use of usable metaphors such as *virtual walls* to control access to contextual data and showed that such metaphors were easy to understand and use. Their work, however, did not address user policies for using such metaphors.

Our work differs from previous work in a number of important ways. Most prior location-sharing studies relied on sampling a couple dozen participants from university populations (largely students). On the other hand, we recruited over one hundred adults spanning a wide age range and geographical area. Furthermore, previous studies typi-

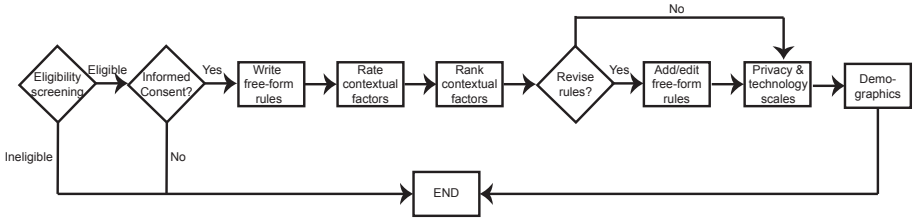

Fig. 1. Flow diagram of the questionnaire.

cally focused on a small set of location-sharing factors sufficient for 'write-once' static disclosure rules. Our study analyzes the absolute and relative importance of a superset of these and other factors. We also performed a detailed analysis of the characteristics of over 200 rules written in free-form everyday language.

3 Method

We used an online questionnaire to investigate the research questions outlined above.

3.1 Questionnaire Structure

Figure 1 shows the flow of the various parts of the questionnaire. The questionnaire asked respondents to write free-form statements describing rules for allowing (or disallowing) access to information about their location via a location-sharing service. We provided four sample free-form rules as illustrative examples. To avoid priming respondents with respect to location-access rules, the example rules dealt with controlling access to an electronic health record (e.g., "Allow a nurse to view my EHR only when I am present in front of her and limit access to the record to the duration of my clinic visit."). Respondents were asked to specify such rules for location sharing. We did not limit the number of rules a respondent could specify. Collectively, these rules formed the respondent's privacy policy for a location-sharing service.

After specifying these rules, respondents were asked to *rate*, on a scale of 1 (Not at all important) to 5 (Very important), the importance of the following factors in determining whether to grant access to location information: (1) *who* will receive the location information, (2) the *reason* for the access, (3) the *time* of the day, (4) the *day* of the week, (5) the user's *present location*, (6) the *specificity* with which location is revealed, and (7) the *number of accesses* within a given period. The factors were presented in random order. We selected these factors because prior studies identified them as important for location-sharing decisions (see Section 2). We were also interested in how these factors are ordered relative to one another. Therefore, we next asked the respondents to *rank* the factors in the order of perceived importance for controlling access to location information.

In order to examine how various individual characteristics of respondents affected location-sharing preferences, the questionnaire also included assessments of the following measures: (1) *Online privacy concern*, which was measured using Internet Users'

Information Privacy Scale (IUIPC) [9], and (2) *Interpersonal privacy concern*, which was measured using a scale from prior studies [7, 12]. In addition, the respondents were asked about their experience using the Internet and smartphones. The questionnaire concluded by collecting demographic information.

3.2 Respondents

The questionnaire was advertised to a subject pool maintained by a university in Pittsburgh,[3] as well as in the Et Cetera Jobs category of the widely-used advertisement site Craigslist. To ensure broad geographical reach across the U.S., we advertised using the Craigslist sites for the cities of Los Angeles, Chicago, Atlanta, and Boston. As compensation, respondents were entered in a drawing for one of five rewards of $15.

Since privacy is culture-dependent, we chose a culturally-homogeneous sample by limiting participation to those who had lived in the U.S. for at least 5 years.[4] Prior research suggests that privacy attitudes and practices of undergraduate students are often different from those of older adults [11]. Therefore, we ensured that no more than 35% of respondents were in the 18–22 age group (i.e., the typical age range of undergraduates). An initial screening questionnaire was used to enforce these criteria.

As a check for detecting whether respondents completed the questionnaire attentively, we included eight 'verification' questions interspersed inconspicuously among other questions. These required the respondents to perform basic mathematical operations (e.g.,"What is 2 + 7?") or follow simple instructions (e.g., "Select option five."). We eliminated from consideration the responses of 31 respondents who did not answer all eight verification questions correctly. We also set browser cookies to reduce the likelihood of multiple submissions from the same respondent.

We received 103 valid questionnaire responses with 21 of these (20.4%) from respondents in the 18–22 range. In the sample 41 (40%) of the respondents were males and 60 (58%) were females.[5] The sample captures a broad age range; the ages of the respondents ranged from 18 through 61 years (median: 28, mean: 32, standard deviation: 12). The respondents were well-educated; 92% ($N = 94$) reported having attended college with 61% ($N = 62$) holding Bachelor's degrees or higher. The respondents also indicated being familiar with technology; 92% ($N = 95$) reported using the Internet for more than 7 years and 68% ($N = 70$) owned smartphones.

3.3 Coding of Free-form Access Rules

The free-form statements written by respondents were coded to mark whether or not the text was a rule for controlling access to the respondent's location. The first three authors acted as three independent coders. The coders also marked whether any of the seven factors that the participants rated and ranked were present in the rules. Further, during the first coding pass, the coders individually identified common themes among

[3] The pool contains a diverse set of individuals from the community and not just university students.

[4] Prior research indicates that sufficient cultural assimilation can be assumed after 5 years [6].

[5] Two respondents did not provide gender information.

the rules. These themes were labeled and agreed upon, and a second independent coding pass was made to mark whether any of these were present in each of the specified rules. The intercoder agreement was high (approximately 82%). All coding differences were collectively resolved until full intercoder agreement was reached. During this process the coders identified 5 respondents who seemed to have misunderstood the instructions (e.g., they wrote rules regarding health records instead of location). The responses of these individuals were removed from the set of valid responses. In the next section we describe the findings from the analysis of valid responses.

4 Findings

We analyzed our coding of the rules the respondents wrote and examined the numeric rating and rankings the respondents attached to the contextual factors we provided.

4.1 Analysis of Free-form Rules

In total the respondents wrote 321 free-form statements. Of these, 234 (73%) were judged as valid rules that could be used for managing access to location information. Notably, 15 (14.6%) respondents did not write a single valid rule (this includes 2 respondents who did not write any rules at all). On the other hand, all of the statements written by 63 (61.2%) were marked as valid rules. However, the number of rules written by most respondents was very small. Of the 88 respondents who wrote at least one valid rule, almost 80% wrote no more than three, with 32 (36.4%) writing one, 22 (25%) two, and 16 (18.2%) three, respectively. The average number of valid rules among the 88 respondents was 2.66/respondent, with a relatively large standard deviation of 2.12.

In addition, the coders identified a few common themes in the 234 valid rules beyond the seven factors we provided (see Section 3). These were:

- **Emergencies:** 26 (11.1%) rules specified permissions for emergency situations.
- **Manual control:** 24 (10.3%) rules reflected a desire for manual control over location sharing. Two types of manual controls were noted: deciding how to handle *each* access for location as it came in (17/234 = 7.3%), and deciding to share location only when explicitly 'checking in' (7/234 = 3%).
- **Do not track:** 37 (15.8%) rules reflected a desire not to have one's locations known or tracked at all. These were further split roughly equally into rules for complete and permanent disabling of location tracking under all circumstances (20/234 = 8.5%) and those for going 'offline' temporarily when desired (17/234 = 7.3%).
- **Current activity:** 15 (6.4%) rules pertained to the activity (e.g., shopping, partying, etc.) the person was engaged in when their location was accessed.

We also noted that two types of recipients—family/friends and the government—were mentioned frequently in the rules, but in contrasting ways. Rules were created to *allow* access to family/friends and to *deny* access to the government. Many respondents did, however, grant location access to the police during emergencies.

Factor	Ranking					Rating					Rules
	N	Mean	SD	Median	Mode	N	Mean	SD	Median	Mode	
Recipient	103	2.07	1.69	1	1	103	4.79	0.68	5	5	175
Where one is when location is accessed	103	3.24	1.73	3	2	103	4.28	0.98	5	5	12
Specificity of disclosure	103	3.68	1.79	4	4	102	4.18	1.01	4	5	12
No. of times location is accessed in a given time	103	4.05	1.61	4	3	103	4.06	1.16	4	5	2
Reason for accessing location	103	4.31	1.70	4	3	102	4.53	0.96	5	5	45
Day of the week	103	5.13	1.51	5	6	103	3.36	1.31	3	3	2
Hour of the day	103	5.52	1.81	6	7	103	3.62	1.23	4	5	9

Table 1. Descriptive Statistics for Ratings and Rankings of Contextual Factors

4.2 Ratings and Rankings of Contextual Factors

Table 1 provides descriptive statistics for the ratings and rankings of the seven contextual factors we provided. The table presents the factors ranked by their mean ranking score. It can be readily observed that most of the factors were rated as highly important when making decisions about location sharing, with modes of 6 out of the 7 factors being 5 (the highest value of importance). However, examining the frequency distributions of the ratings (see Fig. 2) suggests that the ratings did vary. This is also reflected in the differences in the rating means. Pearson's Chi-square test confirmed that the differences were statistically significant (χ^2 = 158, df = 24, p $<$ 0.001).

An exploratory statistical factor analysis suggested a four-factor solution with the following components: (1) recipient and reason for accessing location (*purpose*), (2) one's current location at the time of location access and the specificity with which location is revealed (*location*), (3) time of the day and day of the week (*time*), and (4) the frequency of location accesses (*frequency*). With the exception of the two temporal ratings (i.e., time and day), the ratings also showed a small positive correlation with the level of Internet privacy concern measured by the IUIPC score. The correlation coefficients for the individual ratings ranged between 0.2 to 0.33 and were statistically significant at the 0.05 level or better. In contrast, only the temporal ratings were correlated with interpersonal privacy ratings for non-professional relationships (i.e., significant other, ex, family, and friends). The correlations coefficients ranged between 0.19 to 0.3 and were statistically significant at the 0.05 level.

The rankings in Table 1 shed more light on the relative importance of these factors. The differences in ranking were statistically significant (χ^2 = 395, df = 36, p $<$ 0.001). It can be seen that the recipient of location information and where one is when location is accessed ranked at the top. Moreover, temporal aspects (such as specific times or days) ranked the lowest. The ranking of the factors mostly matched the rank order of mean ratings with one notable exception: the reason behind location access was ranked lower at 5 compared to its rank order at 2 in terms of rated importance.

As mentioned in Section 3, we also coded whether each of these factors was mentioned in the rules written by the respondents. It is seen in Table 1 that roughly 3/4th of all rules (175/234 = 74.8%) were based on specific recipients. Almost 1/5th of the rules

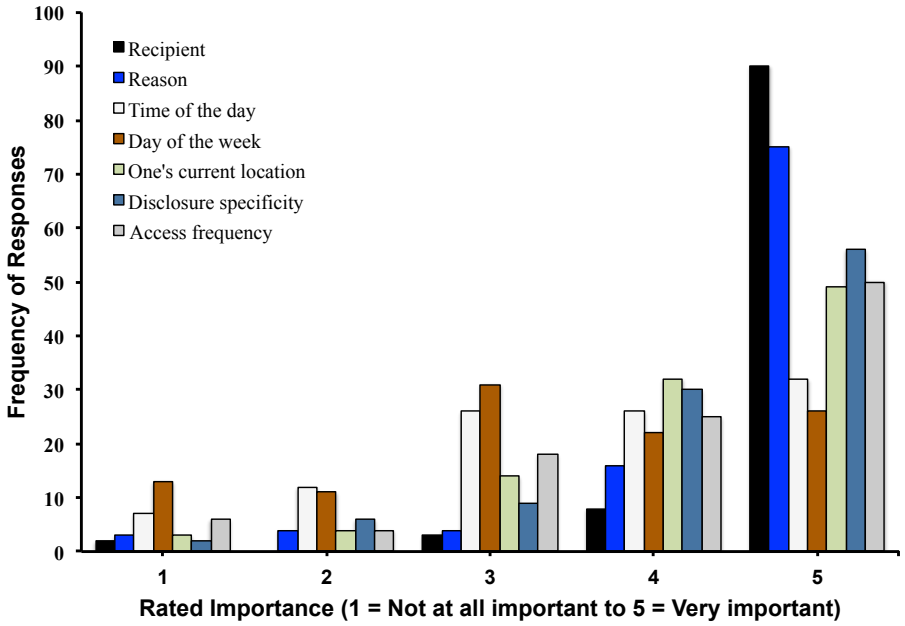

Fig. 2. Frequency Distribution of Ratings for the Importance of Contextual Factors

(45/234 = 19.2%) included specific reasons for location accesses. However, the rest of the factors were mentioned in only a handful of rules, despite being rated and/or ranked high in importance in terms of making location-sharing decisions.

The ratings and rankings did not exhibit any notable impact of smart phone and Internet use, or other demographic factors such as age, income, and education. However, we found that, compared to males, females assigned slightly more importance to the location recipient ($p < 0.05$) and specificity of disclosure ($p < 0.01$).

5 Discussion and Implications

Free-form rule specification: Our findings indicate that people find it challenging to articulate rules describing how access to their location should be controlled. A small but notable group of respondents (14.6%) was not able to do it at all, while most others could only specify one or two rules. As a result, it is likely that the set of rules of a respondent (i.e., the individual's privacy policy for location access) underspecified his or her location-sharing preferences. In other words, most of the contextual factors that were rated and ranked highly by respondents for making decisions regarding location sharing were not captured in their rules. Consider, for instance, the "frequency of location access," which, despite being ranked higher than the "reason for the location access," was only mentioned in 2 rules out of the 234.

We suspect that the difficulties of articulation could be attributed to one or more of the following reasons:

- **Difficulty of 'recall':** It is conceivable that the respondents could not think of all requisite rules in one go. This is reflected in the small number of rules specified by most respondents.
- **Inability or unwillingness to articulate:** Respondents may not have been able to articulate their preferences in the form of a rule and/or may have been unwilling to do so due to the burden imposed by the specification effort. This is also suggested by the respondents choosing not to revise or add to their initially specified rules even though we offered them the opportunity to do so. Only 5 of the 103 respondents revised their earlier rules or specified new rules.
- **Lack of incentive:** It is possible that the respondents lacked sufficient incentive to specify rules because their location information was not at risk during the study or because the compensation offered for study participation was insufficient motivation for putting in the effort.

These considerations point to several possibilities for design explorations to enhance privacy management in location-sharing systems to mitigate the impact of these issues. Users could be provided with lightweight and quick ways to add and revise rules *in situ* at the time of incoming location accesses. The rule set then grows into a comprehensive location privacy policy over time instead of requiring the user to think of every necessary rule at the outset. Moreover, it allows the policy to adapt to situations that the user may not initially have thought of.

The effectiveness of rule specification could also be elevated by an interface that presents important contextual factors for controlling access to location information along with various ways of combining these factors. Such interfaces are typically utilized by email programs for end-user specification of filters for incoming email. Using similar techniques for access-control rules could provide greater flexibility and control than is offered by the typical privacy options in current systems. This may also mitigate the burden of articulation imposed by free-form specification. Templates of important rules can also be included not just to handle commonly expressed desires (e.g., dealing with emergencies) but also to serve as useful initial examples. These rules could be chosen by conducting studies in which users rate and rank various given rules.

Caller ID or Recipient privacy: The dominant importance of the recipient of location information (see Table 1) suggests that it might be useful to provide an incoming 'location call' feature with caller ID. Revealing location in response to a call could then be automated based on pre-specified rules or handled manually by choosing to accept or deny the call. This does, however, present a privacy dilemma: identifying the recipient matches the desires and expectations of those whose location is being accessed (and is aligned with the principle of reciprocity), but hinders the ability of the recipient to anonymously or covertly consume location information.[6] More studies of actual user practices in real-world location-sharing services could shed light on the impacts of enabling or disabling privacy for the recipient.

[6] Note that anonymous or covert location accesses need not be malicious. For instance, an individual's plans for surprising the spouse could require knowing the spouse's location without the spouse finding out that the information was accessed.

Temporal factors: The low relative importance attached to temporal factors is somewhat surprising, as prior research noted the importance of temporal boundaries [13], albeit in a professional context. However, the correlation of temporal factors with desires for privacy from non-professional relations suggests that temporal considerations could be of particular use to those who wish to maintain somewhat distinct personal and professional lives. Traditionally these two spheres have often been temporally separated.

Social, technical, and societal considerations: It is noteworthy that many of the rules seemed to ignore considerations of social nuance (e.g., the connotations of the recipients knowing that they were denied access) as well as technical details (e.g., the possibility of the service provider's records being exposed to hacking or leaks). The rules also expressed desires that may not be easily implementable in purely technical ways. For instance, many respondents expressed a desire to share location during emergency situations. Yet, it is not straightforward to determine what *exactly* constitutes an emergency or to detect such situations automatically. Similarly, preventing access by the government is necessarily intertwined with legal and public-policy considerations. These types of rules likely require *socio-technical* solutions.

6 Limitations and Future Work

It should be noted we sampled only the US population. Since privacy attitudes and considerations vary across cultures, generalizability of these findings to other populations requires empirical verification. Although our sample is diverse in terms of age and geographical reach across the US, it still cannot be considered a representative sample of the US, especially since we recruited participants from two specific sources. The sample is also affected by self-selection bias. Further, the sample size of 103 was too small for adequately analyzing the impact of various demographic factors. Collecting data from additional respondents is necessary to investigate these issues.

In terms of methodology, this is an attitudinal study; self-reported preferences regarding privacy do not always match actual user practice [2]. Moreover, semi-structured interviews might have provided richer details regarding access-control rules than free-form text entries. However, it should be noted that our technique was closer to the specification constraints that users encounter in real-world system implementations.

We are pursuing further research to overcome some of these limitations and to shed more light on user preferences and practices in the new landscape of location sharing. We are currently working on gathering additional data in order to strengthen these findings and conduct more statistical analyses. We also plan to apply the insights to the design of a structured access-rule editor. It would be interesting to study whether rules created using such a tool capture more of the factors deemed important for managing location access. We further hope to expand our exploration to other cultures.

7 Conclusion

We reported the results of an online questionnaire ($N = 103$) that sought to investigate factors influencing people's preferences for location sharing. Location sharing has only recently started gaining mainstream adoption due to the increasing use of smartphones.

Prior work on location sharing, however, has mostly been conducted during the infancy of location-sharing systems. Further, several of the previous user studies were limited in size or scope. In contrast, we reported on a study of a sample of adults in a wide age range (18–61 years) from across the US. We investigated privacy preferences expressed using system-independent, natural language rules. While we confirmed some of the previous findings, we also uncovered new and interesting results that could inform privacy management features of location-sharing systems in today's landscape. For example, we noted that the frequency of accesses is an important factor typically not taken into account by current systems. We also found temporal factors (such as the time of day) to be relatively less important in general, but preferred by those more sensitive to privacy from non-professional social relations. Many contextual factors rated and ranked high in importance consistently failed to show up in free-form access rules. This points to limitations of end-user free-form expression for articulating how access to location information ought to be controlled. The free-form statements did, however, reveal notable insights for managing access to location information. These include special treatment for emergencies, manual control over location disclosure, and turning off location tracking (temporarily or permanently).

8 Acknowledgements

We acknowledge Kristy Caster, Greg Norcie, and Roman Schlegel for help in the implementation and testing of the questionnaire and Tijana Gonja for comments on the analysis. We thank John McCurley for editorial comments on a draft version of this paper. We also thank the study participants for their time and effort. This research is supported by NSF grants CNS-1016603 & CNS-1017229, and US DHS grant 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). The contents of this paper do not necessarily reflect the views of the sponsors.

References

1. Benisch, M., Kelley, P.G., Sadeh, N., Cranor, L.F.: Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs. Personal Ubiquitous Comput. 15, 679–694 (October 2011)
2. Berendt, B., Günther, O., Spiekermann, S.: Privacy in e-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM 48, 101–106 (April 2005)
3. Brodie, C.A., Karat, C.M., Karat, J.: An Empirical Study of Natural Language Parsing of Privacy Policy Rules Using the SPARCLE Policy Workbench. In: Proceedings of the second symposium on Usable privacy and security. pp. 8–19. SOUPS '06, ACM, New York, NY, USA (2006)
4. Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P.: Location Disclosure to Social Relations: Why, When, & What People Want to Share. In: Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 81–90. CHI '05, ACM, New York, NY, USA (2005)
5. Kapadia, A., Henderson, T., Fielding, J.J., Kotz, D.: Virtual Walls: Protecting Digital Privacy in Pervasive Environments. In: Proceedings of the Fifth International Conference on Pervasive Computing (Pervasive). LNCS, vol. 4480, pp. 162–179. Springer-Verlag (May 2007)

6. Khan, R.M., Khan, M.A.: Academic Sojourners, Culture Shock and Intercultural Adaptation: a Trend Analysis. Studies About Languages 10, 38–46 (2007)
7. Kobsa, A., Patil, S., Meyer, B.: Privacy in Instant Messaging; An Impression Management Model. Behaviour and Information Technology forthcoming (2011)
8. Lederer, S., Mankoff, J., Dey, A.K.: Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In: CHI '03 extended abstracts on Human factors in computing systems. pp. 724–725. CHI EA '03, ACM, New York, NY, USA (2003)
9. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15, 336–355 (December 2004)
10. Miluzzo, E., Lane, N.D., Fodor, K., Peterson, R., Lu, H., Musolesi, M., Eisenman, S.B., Zheng, X., Campbell, A.T.: Sensing Meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application. In: SenSys '08: Proceedings of the 6th ACM conference on Embedded network sensor systems. pp. 337–350. ACM, New York, NY, USA (2008)
11. Patil, S., Kobsa, A.: Instant Messaging and Privacy. In: Proceedings of HCI 2004. pp. 85–88 (2004), http://www.ics.uci.edu/~kobsa/papers/2004-HCI-kobsa.pdf
12. Patil, S., Kobsa, A.: Uncovering Privacy Attitudes and Practices in Instant Messaging. In: GROUP '05: Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work. pp. 109–112. ACM, New York, NY, USA (2005), DOI 10.1145/1099203.1099220
13. Patil, S., Lai, J.: Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application. In: CHI '05: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 101–110. ACM, New York, NY, USA (2005), DOI 10.1145/1054972.1054987
14. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J.: Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. Personal and Ubiquitous Computing 13, 401–412 (August 2009)
15. Schlegel, R., Kapadia, A., Lee, A.J.: Eyeing your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy. In: Proceedings of the 2011 Symposium on Usable Privacy and Security (SOUPS) (Jul 2011)
16. Toch, E., Cranshaw, J., Drielsma, P.H., Tsai, J.Y., Kelley, P.G., Springfield, J., Cranor, L., Hong, J., Sadeh, N.: Empirical Models of Privacy in Location Sharing. In: Proceedings of the 12th ACM international conference on Ubiquitous computing. pp. 129–138. Ubicomp '10, ACM, New York, NY, USA (2010)
17. Toch, E., Cranshaw, J., Hankes-Drielsma, P., Springfield, J., Kelley, P.G., Cranor, L., Hong, J., Sadeh, N.: Locaccino: A Privacy-Centric Location Sharing Application. In: Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing. pp. 381–382. Ubicomp '10, ACM, New York, NY, USA (2010)
18. Tsai, J.Y., Kelley, P., Drielsma, P., Cranor, L.F., Hong, J., Sadeh, N.: Who's Viewed You?: The Impact of Feedback in a Mobile Location-Sharing Application. In: Proceedings of the 27th international conference on Human factors in computing systems. pp. 2003–2012. CHI '09, ACM, New York, NY, USA (2009)
19. Wagner, D., Lopez, M., Doria, A., Pavlyshak, I., Kostakos, V., Oakley, I., Spiliotopoulos, T.: Hide and seek: Location Sharing Practices with Social Media. In: Proceedings of the 12th international conference on Human computer interaction with mobile devices and services. pp. 55–58. MobileHCI '10, ACM, New York, NY, USA (2010)