Personality-based Privacy Management for Location-sharing in Diverse Subpopulations

Xinru Page, Alfred Kobsa
Donald Bren School of Information
and Computer Sciences
University of California, Irvine

{xpage, kobsa}@uci.edu

ABSTRACT

Researchers in the area of privacy management often suggest to provide users with a collection of privacy settings and good defaults for them. However, our research into people's attitudes towards location-sharing technology (considering both adopters and non-adopters) indicates that the right way to manage privacy and the right default can vary for different types of people; Key privacy concerns may differ by demographics and personality type, and personality may also influence privacy management preferences. To help researchers and practitioners better understand who is concerned about what, and how to best address those concerns, we will draw on our research and theories in the literature to construct and validate a scale that 1) assesses an individual's main privacy concerns towards location-sharing technology, and 2) measures personality traits relevant to privacy management. We will then put this scale into practice by deploying an enterprise-wide survey at our field site (a large multi-national entertainment corporation) that tests the relationship between the scale/subscales and an individual's intention to adopt location-sharing technology. We hope this will help us identify subpopulations with similar privacy concerns and/or personality traits, which can guide future design of privacy-sensitive location-sharing technology.

Keywords

Location-based service, privacy, personality, demography.

1. INTRODUCTION

Location-based services offer a geo-enhanced way to connect, coordinate, and stay in touch with one's social network. They come both as dedicated applications (e.g. FourSquare, Gowalla, or Loopt), or as part of a larger application (Facebook's Places or Google Latitude in Maps). They allow people to manually check in, continuously share real-time location, and even glean others' locations unbeknownst to them. However, both public media and privacy advocacy groups have pushed back, citing insufficient privacy controls [6]. Addressing privacy concerns is paramount as evidenced by the public outcries when Facebook put users' status front and center in their friends' news feeds and when Google Buzz auto-generated and made public ones' follower list.

Smart phones capable of location-sharing rapidly increase in number, and location-sharing features increasingly infuse social and work-oriented applications. Our challenge is to strike a balance between utility and privacy of such services. To do this we must better understand privacy attitudes towards location-sharing technologies, particularly for demographics not commonly represented in the research literature.

iConference 2011, February 8–11, 2011, Seattle, WA, USA.

2. RELATED WORK

Location-based services have been slow to infiltrate mainstream social media adoption [3]. Research therefore has emphasized exploring attitudes towards hypothetical scenarios [12] or recruited participants using location-sharing prototypes [1]. Research into privacy management has ranged from computational algorithms (e.g. anonymity, obfuscation) [4] to helping users specify their preferences [10] and offering good defaults [11]. Privacy scales often focus on data protection [5].

As commercial location-sharing services have become more popular, we have been able to bridge a gap in the literature [2] by studying post-collegiate *non adopters* and *adopters* of location-sharing in social media [7,8]. These studies suggest that various types of social pressures due to inappropriate system design may be the biggest source of privacy concern, preventing people from regulating boundaries the way they'd like (cf. [9]). Moreover, better design may be personality-based.

3. METHODOLOGY

3.1 Model

It is important for researchers and practitioners to understand whether users will engage in location-sharing technology and under which contexts. Thus we will hypothesize a model for predicting intention to engage in the technology. To this end, we will identify key privacy concerns, contexts of use, and personality factors based on a new analysis of our previously conducted exploratory studies of non-adopters and adopters of location-sharing technology [8]. To elicit key privacy concerns outside of our demographic, we will perform a literature review of privacy in location-based services and add to the previous list of concerns. We will then construct a model illustrating the relationship between these constructs.

We will also account for covariates such as demographics known to affect privacy attitudes (e.g. sex, age, education) as well as new factors coming out of our research (e.g. marital/relationship status, social networking use).

3.2 Scale creation

We will operationalize the constructs in the model by building a scale consisting of two major components – one portion assessing an individual's major privacy concerns, another assessing

This research has been supported by NSF Grants 0831526 and 0953071.

personality traits. In both we ensure content validity by drawing from qualitative data in our prior research to create Likert scale items that represent each construct (e.g. a feeling like "I share my location because everyone else does it" would represent the normative pressure to disclose location). Thus we will have subscales for each privacy concern and personality trait focused on privacy in the context of location-sharing technology. We have chosen to use subscales for each construct (rather than just combining them into an overall privacy concern measure) so that we can evaluate the relative importance of each.

3.3 Scale validation

In order to test the scale and identify the new factors, we will construct a structured online survey and administer it to a random sample of 400 employees taken from the full employee population in both U.S. west coast and east coast regions of a large multinational entertainment corporation.

Convergent and Discriminant validity. To check convergent and discriminant validity, we will include scales from the literature for a similar or dissimilar construct alongside each subscale. For example, a social conformity scale would be used alongside our subscale measuring whether individuals succumb to social pressure to disclose location. This enables us to check that they correlate highly for convergent validity.

Pilot. We will pilot the survey with our initial interview subjects as well as a new pool of subjects. The former allows us to match their responses with the personality profiles and privacy concerns we originally derived from their interviews. The latter allows us to check for clarity from a fresh perspective. In both we will check for internal consistency since we will use multiple measures for each construct.

Deployment. The field site was chosen because it represents a wide variety of people, from teenagers to retiree-aged employees performing white and blue-collar work at all levels of the company and in assorted business sectors including sales, finance, food services, internet, and entertainment. For this study we exclude international employees since our initial research is focused on individuals in the U.S. while privacy is influenced by culture. Because the survey will be one of a few yearly tasks required of employees, we expect a high response rate. Past experience shows that the response rate will be in the 90% range.

Determining Factors. Based on the survey results, we will perform an exploratory factor analysis to discover which constructs emerge as independent factors. The items with high factor loadings will be retained. The remaining items will be used in the hypothesis-testing phase.

3.4 Hypothesis testing

We will next turn to testing our model and concurrent validity using a scenario-creation method similar to that used for other privacy scale validations [5]. Because we anticipate different attitudes towards location-sharing technology as the context of use (e.g. carpooling for work, social connection, etc.) and the type of available privacy management features varies, we will create scenarios representing each combination. Subjects will be presented with all of the scenarios, signing up for the location-sharing technology variations they are willing to use (each scenario produces a binary dependent variable). Thus, this will be a repeated measures factorial experimental design instead of a between subjects design which allows us to increase the number of scenario choices for our analysis. After subjects respond to the scenarios, they will receive the survey from the previous step and items representing the covariates (see Section 3.1).

We will administer this complete survey to a new sample of employees drawn from our field site (N>=1000). First we will perform a confirmatory factor analysis on the new survey results to check for good measurement model fit of our scale, dropping items and rechecking the new measurement model as needed. We will also check for convergent and discriminant validity in the new data for the items previously identified during the initial scale validation. After checking the scale, we can proceed to test the hypothesized model with structural equation modeling.

4. Conclusion

This scale can be a tool for better understanding privacy concerns and privacy management preferences in a diverse population. We will use it to guide future research into building and designing location-sharing technologies for various subpopulations, which we will also test at this field site.

5. REFERENCES

[1] Barkhuus et al. (2008). From awareness to repartee: sharing location within social groups. In *Proc. CHI 2008*, Florence, Italy: ACM, p.497-506.

[2] Boyd, D.M. & Ellison, N.B. (2007). Social Network Sites: Definition, History, and Scholarship. In *Journal of Computer-Mediated Communication*, vol. 13, p.210-230.

[3] Kickuhr, K., & Smith, A. (2010). 4% of online Americans use location-based services. Pew Internet & American Life Project.

[4] Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiq. Computing*, *13*(6), 391-399.

[5] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Info. Sys. Research*, *15*(4), 336-355

[6] Ozer, N.(2010) Facebook Places:Check This Out Before You Check In http://www.aclunc.org/issues/technology/blog/facebook_places_check_this_out_before_you_check_in.shtml

[7] Page, X., Kobsa, A. The Circles of Latitude: Adoption and Usage of Location Tracking in Online Social Networking. *CSE 4*, (2009), 1027-1030. doi: 10.1109/CSE.2009.195

[8] Page, X., Kobsa, A. Navigating the Social Terrain with Google Latitude. In *Proc. iConference 2010*. http://hdl.handle.net/2142/14951

[9] Palen, L. & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In *Proc. CHI 2003*, p.129-136.

[10] Sadeh et al. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, *13*(6), 401-412.

[11] Toch, E., Sadeh, N. M., & Hong, J. (2010). Generating default privacy policies for online social networks. In *CHI 2010 Extended Abstracts*, Atlanta, Georgia, p.4243-4248

[12] Tsai et al. (2010): Location-Sharing Technologies: Privacy Risks and Controls. I/S: A Journal of Law and Policy for the Information Society, Summer 2010