Privacy in location-based social networks: Researching the interrelatedness of scripts and usage

Paulien Coppens, Laurence Claeys, Carina Veeckman and Jo Pierson

iMinds-SMIT,Vrije Universiteit Brussel
Pleinlaan 9
1050 Brussels, Belgium
Paulien.Coppens@iminds.be

ABSTRACT

With the increasing adoption of smartphones, location-based social networks and applications gain widespread popularity. However, the disclosure of location information within these networks can cause privacy concerns among mobile users. In most of the research on privacy in location-based social networks, technology is researched as a context factor for explaining privacy related behavior. In our study, we take a post-phenomenological ontological position and we translate this into our empirical research using the Science & Technology Studies perspective on the relation between technical scripts and user practices. Following the work of Madeleine Akrich (1992), we study the privacy scripts in two location-based social networks. In a qualitative user study, we research their framework of action and how they shape privacy concerns and practices.

1. INTRODUCTION & BACKGROUND

Mobile phones are personal and influential artifacts in the everyday life of many people, which leads to an 'embodiment relation' with the communication device [11]. At the same time smartphones are getting smarter and more sophisticated every day, being able to capture very precise contextual data (e.g. movement, orientation and location) of the user. Developers integrate these data sources into different mobile applications, hereby stimulating the growth of different types of location-based social networks (LBSN) such as Foursquare or Find My Friends. But the integration of location data within these applications also brings along new privacy concerns. Although privacy issues are not a recent concern of users, they become more pronounced in the mobile environment where (usage) context and activity are mutually constituent in 'embodied interactions' [9]. In the mobile context, it is relevant to point to two of the elements of location privacy as identified by Ardagna et al. [2]: position privacy, which refers to the protection of the user's position, and path privacy or the protection of the location movement of a user who has been monitored for a longer period of time. Earlier research found that location-tracking services (path privacy) cause higher privacy concerns than position-aware services [3]. A higher perceived control over personal data can, however, help in decreasing privacy concerns [4,8,13,16,18,20]. If the technical control features (e.g. privacy settings) to limit the visibility of personal information do not suffice, users sometimes apply their own strategies to deal with possible (location) privacy issues. This is illustrated in the user study of Boyd and Marwick [6], who found that teens on social networking sites on the one hand apply social strategies in which they limit the meaning of their messages to make them incomprehensible for unwanted people or parties (e.g. social steganography). On the other hand, they can also apply 'innovative structural strategies for achieving privacy that don't rely on Facebook's privacy settings' [6:20]. The study of Boyd & Marwick nicely demonstrates the interaction between the technology and the user, which is studied in The Science & Technology Studies (STS).

The STS domain states that multiple contextual factors define the interplay between the technology and user, or as they call it: the mutual shaping process between technology and society [5]. Instead of focusing on the technical features, STS investigate how technologies are socially, culturally, historically, economically, and/or institutionally shaped [10]. There is no strict division between the technology and the user as they exist only in an interrelational way, whereby each part of the interrelation is mutually depending upon the others for the emergence of understanding [12]. A technology can shape a framework of action, but users might also use the technology in a way not foreseen by the designer [1]. Madeleine Akrich [1] refers to this framework of action, or the preferred reading of users' behavior, as the *script* or the scenario of a technology. The design of a technology defines which decisions can be made by the user and what is controlled by the 'machine'. Technologies can shape users' practices, the space in which users are supposed to act and the ways in which they interact. However, in their interaction with the technology, users can also adopt the technology in their everyday life in another way than envisaged by the designer. We can also apply these insights to study privacy concerns for media technologies, and in the context of this paper, to the study of LBSN users' (location) privacy concerns. To explore how these concerns can guide privacy practices, we have to scrutinize the LBSN and how the preferred user behavior is inscribed or scripted into these technologies. Users nowadays make privacy decisions in a rather untransparent market. In their search for creating a good user experience and a valid business model, different location-based service providers embed the user location sharing practices into their applications in different ways. Mobile applications have in them a preferred reading of the information

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

sharing behavior of the user, e.g. by means of the default privacy settings, or as Palen and Dourish [14:8] describe it: 'The privacy management process takes place in the context of the possibilities that are offered by one or another technology*'.*

The privacy scripts of mobile applications are not yet widely explored in previous privacy studies. Following the work of Akrich [1], we study the scripts of LBSN and how users' privacy concerns exist within the framework of action of these scripts. We have set up a qualitative study to gather insights on and to illustrate the importance of the mutual shaping process of technology and usage on the topic of location privacy.

2. METHOD

The study consists of two parts: a comparative analysis of the privacy scripts of two commercial LBSN and a qualitative user study in which we study how the privacy scripts of these LBSN shape privacy concerns.

2.1 Comparative script analysis

The embedded privacy scripts of two LBSN, namely Foursquare[1] and Glympse[2], are analyzed in a comparative way. Foursquare is a social-driven check-in service, allowing users to share their location among a large network of friends. By checking-in, users can collect points or badges, unlock local deals and read or leave tips on a variety of locations. In contrast, Glympse is a purpose-driven location-tracking service that allows users to let one, a few or a large group of person(s) follow their location movement for a defined period of time. These two applications were chosen because of their different privacy scripts, but also because they represent different categories of location-based services. Contrary to purpose-driven LBSN, social-driven LBSN 'emphasize the social aspects of location sharing, where users might announce their arrival at a location not because others *need* to know but because it is simply interesting or fun to do so' [17:1].

The LBSN are compared on 4 levels. First, the personal information necessary to register for or use the application, information that can be accessed by other people using the LSBN or by third parties. Second, the default privacy settings, or the privacy settings as they are preset by the application provider. On the one side of the spectrum, there is the situation where the user has full control over the privacy settings and the settings are preset in favor of the privacy of the user. On the other side of the spectrum, the user has no or little control over privacy settings and the default settings are set to maximize the sharing of personal data. Third, the configuration possibilities of the LBSN, or how much sharing options the user has each time he or she wants to share a location (e.g. with one, a few or a group of people). Finally, we also scrutinize the privacy policies of both Foursquare and Glympse.

2.2 User study

Although a survey is a valuable instrument to study privacy concerns, it is less suitable in capturing the interplay between the technology and the user and how the privacy script of a technology affects these privacy concerns. We therefore opt for a qualitative post-phenomenological research approach in which we study the real-life use of two existing LBSN. The two different categories of LBSN make it interesting to explore how privacy strategies, along with the privacy scripts, differ among the mobile applications and their different usage motivations.

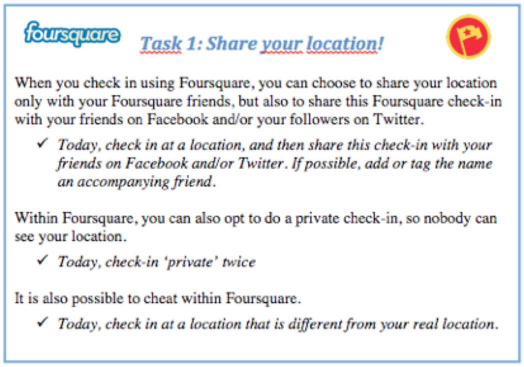
Given the in-depth and intensive nature of our study, a small group of participants were involved (n=9). The participants were recruited based on an online questionnaire, sent to a panel of smartphone and mobile Internet users located in Flanders, the northern part of Belgium (n=2,302, April 2013).[3] Questions asked about mobile phone behavior, usage of location-based services and privacy attitudes. The survey helped us in purposefully selecting the right mix of respondents (mix privacy concerned and unconcerned users, mix experienced and non-experienced LBSN users) and gave us background information on the. All respondents were between 22 and 35 years old and 5 male and 4 female respondents participated. With the exception of one participant, the participants took part in the study in teams of two. This way, at least one person in the users' social circle used the application as well, stimulating the real-life use of the LBSN. Data were collected between September and October 2013.

The study consisted of three consecutive phases. First, an interview was conducted to get to know the participants and to reflect with the respondents upon their smartphone and LBSN usage. The study was presented and we helped with and observed the installment of the applications on the participants' own mobile phone. The interview was followed by a three-week field trial, in which the participants were asked to use the two LBSN by fulfilling some predefined scenario tasks whereby triggering users' location privacy awareness was central. In the first week the participants got familiar with both applications, and explored the different functionalities by completing some small tasks (e.g. check in at a venue using Foursquare and leave a tip). In the next two weeks, we included three tasks for each LBSN to encourage the respondents to explore and investigate the (default) privacy and location settings of the applications (see figure 1). To keep track of their practices and to gather some first impressions, participants were requested to fill in a short (logging) questionnaire at the end of each week. Finally, after the field study, we did in-depth interviews with the participants, which took on average one hour to one hour and a half per interview. Here, the different scenario tasks were discussed and the users' privacy management and concerns were discussed for both applications. To not influence the participants' privacy concerns or evoke explicit privacy (non-)protective behavior, participants were not informed about the 'privacy goal' of the study.

[1] https://foursquare.com/

[2] http://www.glympse.com/

[3] The in this paper described qualitative study is part of bigger research project in which we explore mobile users' location privacy experiences. We can here fore rely on a large panel of over 5,000 smartphone and mobile Internet users located in Flanders, the northern part of Belgium. The first online survey (n=2,302, April 2013) and the qualitative study (n=9, September-October 2013) gave input for a second online questionnaire in which LBSN users' willingness to share location information was quantitatively explored, hereby including privacy concerns as a primary influencing factor (n=909, December 2013). See also: [19]



foursquare **Task 1: Share your location!**

When you check in using Foursquare, you can choose to share your location only with your Foursquare friends, but also to share this Foursquare check-in with your friends on Facebook and/or your followers on Twitter.

- ✓ *Today, check in at a location, and then share this check-in with your friends on Facebook and/or Twitter. If possible, add or tag the name an accompanying friend.*

Within Foursquare, you can also opt to do a private check-in, so nobody can see your location.

- ✓ *Today, check-in 'private' twice*

It is also possible to cheat within Foursquare.

- ✓ *Today, check in at a location that is different from your real location.*

Figure 1. Field trial - Foursquare task 1

Results were gathered on an individual basis, although the interviews were done per team of two. In this way the respondents could critically assess each other's behavior during the interviews. Organizing the interviews per team also gave us the advantage to collect additional insights on location sharing practices among social ties.

All results were analyzed using the NVIVO 10 software for qualitative analysis. All files (survey data, logging questionnaire, the fully transcribed intake and closing interviews) were included into the software and coded, based on the open and closed coding technique [15].

3. STUDY RESULTS

3.1 Privacy scripts

The comparative analysis of Foursquare and Glympse reveals different privacy scripts for the two LBSN. First, Foursquare requires a lot of personal information to make use of the service, whereas this is not the case for Glympse. Users also have limited control over the display of their personal data within Foursquare. The different usage goal of the applications partly explains why Foursquare requires more personal data. Foursquare is a social-driven application in which the creation of a social network is central, whereas this is not the case for the purpose-driven location sharing within Glympse. Next, when looking at the default privacy settings of Foursquare and Glympse, we can situate them at other sides of the spectrum. Within Foursquare, users have control over a rather small amount of privacy settings and, except for one privacy setting, the default settings all preset personal data as public (e.g. photos added to check-in). Glympse, on the other hand, has no privacy settings section. Each time the user wants to share a location, he can control with whom the location is shared (one person, multiple people, group), for how long and until which destination. Glympse users thus have elaborate configuration possibilities, whereas Foursquare does not offer their users these possibilities. Location is by default shared with all your Foursquare friends. Finally, we compared the privacy policies of both Foursquare and Glympse. Both policies are similar, but Foursquare makes an extra effort to make the privacy policy a bit more transparent. In addition to the privacy policy, they offer a document that describes in an easier and more concise way the main topics in the privacy policy and they provide a set of FAQs related to privacy.

The analysis of the privacy scripts of Foursquare, a check-in service, and Glympse, a location tracking service, shows that the two LBSN have a different privacy script. Glympse is an application designed to give users almost full control over their location sharing settings. Foursquare on the other hand, defines another framework of action for the user. It appears to be in the interest of the Foursquare application, contrary to Glympse, that as many personal data or settings as possible are set as public. For a rather big set of data, users have no possibility to set it as private and the privacy settings that are adjustable are set public by default. A possible explanation for this is the fact that Foursquare works together with local businesses and brands that have access to aggregated and anonymous data. We could thus say that, contrary to Glympse, the preferred reading of Foursquare limits users in the management of their personal data.

3.2 Mutual shaping between LBSN and location privacy

The user study focuses on how the privacy scripts of Foursquare and Glympse can shape participants' privacy concerns and practices and on users' coping mechanisms in redefining this framework of action.

The comparative analysis of the privacy scripts reveals that Glympse is a more privacy preserving LBSN. However, the respondents perceive Glympse to be more privacy-invasive than Foursquare. Glympse is a location-tracking service, causing higher privacy concerns than the position-aware service Foursquare. On top of that, we also have to take into account the control factor. Although the analysis of the privacy scripts shows that Glympse gives users more control mechanisms (e.g. control over audience), most of the participants feel they have a higher control over the disclosure of their location when using Foursquare. Important here, contrary to actual control, is thus the notion of perceived control or the "illusion of control" [7]. Within the check-in service Foursquare, users can each time make the conscious decision to share a specific location, while within Glympse a longer location path is shared.

When taking a closer look at the participants' practices, we can see that, although the importance of control over location data is continuously stressed, they do not always act upon this. Some of the participants did not know which information was displayed on their Foursquare profile (e.g. telephone number) and we were surprised to find that most of the participants had never looked at their Foursquare privacy settings before. A possible explanation for this - in line with Foursquare's privacy script - is that the privacy settings are hidden somewhere in the background of the application, and therefore not easily checked. However, we should also note that when a LBSN does not offer enough control features to protect location information, the respondents sometimes apply very inventive strategies to protect their location. An example here is a participant who reports to never check in with Foursquare every day and/or at the same time at work and at home to make it difficult for someone with malicious intents to discover daily routines. This example nicely illustrates the interplay between on the one hand the technology and the accompanying privacy script, and on the other hand users' practices. In dealing with their privacy concerns, the respondents take control upon themselves and use the technology in an unforeseen way. In general, the most important way respondents try to protect location information is to always thoughtfully consider whether or not to share their location. If they do not want others to know their location, they just do not share it.

Although control is considered important in decreasing privacy concerns, the trade-off between more control and the ease of use of an application has to be made. Some respondents reported they would never use Glympse in everyday life because the effort to each time define the sharing settings is too big. We also showed mock-ups of other applications with more advanced location privacy settings and configuration possibilities (e.g. defining fine-grained location-sharing rules) to the respondents, but these were also considered too elaborate.[4] Although respondents say they want full control over privacy settings, our study shows that they are not willing to each time define elaborate sharing settings. This also continuously makes the process of sharing personal information more visible for users and users do not always like to be confronted with that. It is a challenge for LBSN providers to find the right balance between privacy-preserving affordances and an optimal user experience.

4. DISCUSSION AND CONCLUSION

In this paper we illustrated from an STS perspective how we can take into account the interplay between the technology and the user within privacy research. For this, one needs to scrutinize technologies and their privacy script in shaping users' privacy concerns and practices. We opted for a qualitative research approach consisting of three phases in which we combined in-depth interviews, observation and short (logging) questionnaires. We asked respondents to use two existing and commercialized LBSN, Foursquare and Glympse, making it able for the respondents to include their own social network in the application. The usefulness of this approach for our research goals lies in its value to reflect upon the usage of LBSN in a natural 'in situ' environment, making it possible to study users' actual privacy practices and concerns. This has some advantages over studies which rely on hypothetical scenarios, in which the respondents may have lower privacy concerns because location sharing holds no risk, or higher concerns because the sharing is not rewarded with (social) benefits [17].

Our study shows that Glympse responds to mobile users' privacy concerns by giving them more options to control the disclosure of location information. Foursquare defines another framework of action for the user. It appears to be in the interest of Foursquare that users provide many personal data that are set as public. This is illustrated, among others, by the fact that, although all the respondents want high control over the (location) privacy settings, almost none of them ever checked the Foursquare privacy settings before. However, when thoroughly investigating the usage, users consider Foursquare to be less privacy invasive than Glympse. This is partly due to the properties of the LBSN. Glympse is a location-tracking service, which decreases the respondents' feeling of control. But also to the fact that the check-in service Foursquare makes it easier for the respondents to apply their own strategies to control location disclosure, hereby opposing the application's framework of action.

In future research, it might be interesting to study the privacy scripts of a wider selection of LBSN, and the differences within and between the different categories of LBSN, among a wider variety or respondents (age range, experience with LBSN, privacy attitudes and behavior).

To conclude, we wish to stress that how a technology is used will be influenced by what the technology enables. Future privacy studies should more often incorporate the interplay between the technology and the user. Users might use the technology in a way not foreseen by the designer, 'but as long as the circumstances in which the device is used do not diverge to radically from those predicted by the designer, it is likely that the script will become a major element for interpreting interaction between the object and its user*'* [1].

5. ACKNOWLEDGMENTS

This research project has been supported by the Flemish Agency for Innovation by Science and Technology through the ICON-project SoLoMidem (http://www.iminds.be/en/projects/2014/03/18/solomidem) and by the European Commission under the 7th Framework Programme through the USEMP project (Grant agreement no. 611596) (http://www.usemp-project.eu)

6. REFERENCES

[1] Akrich, M. The description of technical objects. In W. Bijker and J. Law, eds., *Shaping technology/building society: studies in sociotechnical change*. MIT Press, Cambridge, MA, 1992, 205–223.

[2] Ardagna, C.A., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., and Samarati, P. Privacy-enhanced location services information. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. De Capitani di Vimercati, eds., *Digital privacy. Theory, technologies, and practices.* Auerbach Publications (Taylor & Francis group), Boca Raton, 2008, 307–326.

[3] Barkhuus, L. and Dey, A. Location-based services for mobile telephony: a study of users' privacy concerns. *Proc. Interact*, Citeseer (2003), 709–712.

[4] Benisch, M., Kelley, P.G., Sadeh, N., and Cranor, L.F. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing 15*, 7 (2011), 679–694.

[5] Bijker, W. and Law, J. *Shaping Technology/Building Society: studies in socio-technical change.* MIT Press, Cambridge, MA, 1992.

[6] Boyd, D. and Marwick, A. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. (2011).

[7] Brandimarte, L., Acquisti, A., Loewenstein, G., and Babcock, L. Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis. (2009).

[8] Brandimarte, L., Acquisti, A., and Loewenstein, G. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, (2012).

[9] Dourish, P. What we talk about when we talk about context. *Personal Ubiquitous Comput. 8*, 1 (2004), 19–30.

[10] Gillespie, T., Boczkowski, P.J., and Foot, K.A., eds. *Media Technologies: Essays on Communication, Materiality, and Society*. MIT Press, 2013.

[11] Ihde, D. *Technology and the lifeworld. From garden to earth.* Indiana university press, Bloomington, 1990.

[12] Ihde, D. Forty Years in the Wilderness. In E. Selinger, ed., *Postphenomenology: A Critical Companion to Ihde*. SUNY Press, Albany, NY, 2006.

[4] The LBSN of which the privacy settings and configuration possibilities were demonstrated, were PCube (http://www.everywaretechnologies.com/apps/pcube) and Locaccino (http://locaccino.org).

[13] Lin, J., Xiang, G., Hong, J.I., and Sadeh, N. Modeling people's place naming preferences in location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing*, (2010), 75–84.

[14] Palen, L. and Dourish, P. Unpacking privacy for a networked world. *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM (2003), 129–136.

[15] Strauss, A. and Corbin, J. *Basics of Qualitative Research. Grounded Theory Procedures and Techniques*. Sage, Newbury Park, 1990.

[16] Stutzman, F., Capra, R., and Thompson, J. Factors mediating disclosure in social network sites. *Computers in Human Behavior 27*, 1 (2011), 590–598.

[17] Tang, K.P., Lin, J., Hong, J.I., Siewiorek, D.P., and Sadeh, N. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing*, ACM (2010), 85–94.

[18] Toch, E., Cranshaw, J., Drielsma, P.H., et al. Empirical models of privacy in location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing*, (2010), 129–138.

[19] Veeckman, C., Claeys, L., Coppens, P., Verbrugge, K., and Stevens, I. Mobile users concerns for information privacy in location based services. (2014).

[20] Xu, H. The effects of self-construal and perceived control on privacy concerns. *Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007)*, (2007).