Tensions in Developing a Secure Collective Information Practice - The Case of Agile Ridesharing

Kenneth Radke[1,2], Margot Brereton[1], Seyed Mirisaee[1], Sunil Ghelawat[1], Colin Boyd[2], and Juan Gonzalez Nieto[2]

[1] School of Design, [2] Information Security Institute,
Queensland University of Technology, Australia
{k.radke, m.brereton, s.mirisaee, s.ghelawat, c.boyd, j.gonzaleznieto}@qut.edu.au

Abstract. Many current HCI, social networking, ubiquitous computing, and context aware designs, in order for the design to function, have access to, or collect, significant personal information about the user. This raises concerns about privacy and security, in both the research community and main-stream media. From a practical perspective, in the social world, secrecy and security form an ongoing accomplishment rather than something that is set up and left alone. We explore how design can support privacy as practical action, and investigate the notion of collective information-practice of privacy and security concerns of participants of a mobile, social software for ride sharing. This paper contributes an understanding of HCI security and privacy tensions, discovered while "designing in use" using a Reflective, Agile, Iterative Design (RAID) method.

Keywords: Usable privacy and security, user experience based approaches, trust, design, HCI, participation.

1 Introduction

The growth in use of tracking and data mining technologies, in order to support human activities, increasingly raises concerns about privacy and security. In this paper we explore how to address these issues through a case study of agile ridesharing, in which we are investigating how to grow the practice of ad hoc shared vehicle rides arranged in real time through mobile social software. Ridesharing software stands to benefit from tracking and data mining technologies, but the decision of whether to share information and share rides is inherently situated in social and cultural perspectives. Dourish and Anderson argue for a move away from narrow and technically focused views of privacy and security toward a holistic view of situated and collective information practice [7]. Here, we attempt to build on this view by exploring how to evolve a secure collective information practice in the ongoing design of a successful ridesharing system.

In explicating the need to consider collective information practice, Dourish and Anderson [7] consider alternative views:

- Privacy as economic rationality – the trade-off between risk and reward;
- Privacy as practical action – the practical detail of what people do to maintain privacy; and
- Privacy as discursive practice – the way in which notions of privacy and security are used to categorize activities, events and settings, separating acceptable actions from unacceptable ones.

In defining collective information practice, Dourish and Anderson argue for a greater focus on the latter two approaches, explaining that rational actor economic models "are inadequate as sole explanations of privacy and security practices because they fail to capture other symbolic and social values." Further, various studies have shown that humans do not make use of such rational decision making with respect to privacy and security [19,1]. Dourish and Anderson explain collective information practice as "collectively reproduced understandings of the ways information should be shared, managed and withheld."

The shift from privacy and security as disconnected and abstract technical practices, that can be setup and left alone, to ones that are performative, ongoing accomplishments, calls into question the separation between configuration and action that characterizes most interactive systems for privacy and security management. A collective information approach posits *how can configuration and action be achieved together and collectively evolved*?

However, the story is complicated by the issue of technical infrastructure [20,2], because social and mobile software applications for ridesharing typically need to operate across existing internet based technical infrastructures, where security is protected under a model of risk and reward. Given this situation, we pose the question, "What is a practical way to evolve a collective information practice for ridesharing building on existing infrastructures?"

The approach that we propose is firstly a methodological one, drawing upon a reflective agile iterative development (RAID) method to grow a ridesharing culture, where the practicality of security can be devised collectively in the doing. Secondly, we examine the tensions in the existing approaches wherein technical capabilities may go beyond, be insufficient for or introduce conflicts with human needs, and explore how we might resolve these through evolution of collective information practice.

Table 1 – Tensions between Technical and Cultural Practices

Technical practices		***Cultural practices***
Precise Tracking	versus	Imprecision (negotiated and necessary disclosure)
Prior information disclosure and setup	versus	Action over time and in the moment
Moderation	versus	Referral and reputation
Underlying infrastructure databases etc	versus	Accountability and transparency

A potential reason for the difference between technical practices and cultural practices, outlined in Table 1, is the disparity between the necessary probabilities of success for a cyber attack, compared with an attack in a social environment. Taking a rational economic view, an attack in a social environment (such as a robbery) may need a success rate of, at least, one in ten to be worthwhile for the perpetrator; whereas in the cyber-world a one-in-a-million attack can be seen as successful [17].

Privacy and security are a pervasive aspect of how a system is designed and they cannot simply be grafted on [7]. We propose that, from a practical perspective, in the social world, security is an ongoing accomplishment rather than something that is set up and left alone, in agreement with Dourish and Anderson. However, it was not clear how a design approach can work to support the ongoing accomplishment of security and privacy. In this paper we examine a design case study in order to explore how design can support privacy as practical action.

2 Background

Agile ridesharing aims to utilise the capability of social networks and technologies such as mobile phones and web applications, to facilitate people sharing vehicles and journeys. Social technologies, such as SMS, email and web applications, provide the opportunity for people to offer and request impromptu rides in real time.

Previously, most mobile phone and social-network-supported ridesharing, such as Zimride, Avego and GoLoco has been limited, due to being based on a particular phone or social network platform, due to insufficient ride matches, and due to following a standard carpooling paradigm of regular shared rides which is impractical for many people in many circumstances. An investigation of existing rideshare approaches, in 2009, identified that there was a need, and potential based on new technologies, to create a system which allowed people to, in real time rather than a static matching program, arrange ride sharing based on extended social networks [4].

3 Related work

The range of social network designs, all with privacy and security issues, is very broad. Some examples are covered by the empirical work by Patil and Lai, who investigated the privacy settings of MySpace users [13]. Privacy is generally approached as a social consideration, whereas security is seen as a technical concern, though they are closely related [7]. We argue that technical security decisions in the interface and underlying infrastructure of internet communication have such an impact on privacy, that privacy needs to be considered from the perspective of the technical infrastructure and interaction with it, in order to ensure that the privacy expected from the social perspective is achieved. While we do not retreat from attempting to better support privacy as ongoing practice, the practicalities of interaction and design with technical infrastructure also need to be addressed.

Lampe, Ellison and Steinfield, in their study of 1085 Facebook users which explored users' expectations of privacy, also made important contributions in the exploration of users' expectations [12]. They found that 90% of participants believed that no one from outside their university would read their Facebook page, and that 97% of participants believed that no law enforcement agency would look at their Facebook page.

Schechter et al. created a study in which bank websites were progressively changed, to become less and less secure, and the researchers determined whether the participants continued to enter their passwords into the website (which they did) [15]. Similarly, De Keukelaere et al. and Sotirakopoulos et al. examined the effectiveness of security warnings, and their work provides succinct credible information that users were largely untrained in security and would not notice shortfalls in security [6,18].

The conclusion is that privacy must be designed in, and that the default privacy settings both need to be sufficient to ensure the expected privacy, without user education and input, and sufficient to allow the socio-technical system to work effectively, which creates a tension. Sasse et al. argued that existing HCI techniques are sufficient to address security issues in the design of systems [14]. This being the case, it is important that the critical questions and concerns are identified. Our study outlines the range of security and privacy issues identified in an ongoing, location-specific, social networking application and draws attention to particular tensions.

4 Iterative “design in use” approach

From a methodological perspective, figuring out how to accomplish *privacy and security in the doing* points toward an approach that combines ethnographic study and iterative design. For this reason our agile rideshare project has adopted a reflective agile iterative development (RAID) method to explore the design requirements for an agile rideshare system [10].

In summary, the design approach aims to:

- Understand community practices through ethnographic fieldwork
- Explore key design hypotheses by designing and deploying working investigatory prototypes for use by a segment of the community;
- Gather fragments of ethnographic data from the prototype in use;
- Build communities of use as the prototype is refined and extended;
- Understand the factors that persuade or dissuade others from joining.

The approach uses the simplest functioning technology prototypes deployed over an extended period, to understand how people use them in their daily lives to augment their activities. Thus the approach emphasizes understanding of use over feature provision and the functionality is extended in order to address pressing needs and emergent opportunities. We have employed a gradual growth strategy, as is recommended to ensure successful customer interaction [5], and in order to ensure due consideration is given to these issues.

The rideshare prototype was initially developed for use among a small group of people who knew each other in order to understand basic aspects of the interaction paradigm, as reported in [9]. Following use of the simple prototype this group was able to consider practical aspects of sharing, privacy and security through use, and to consider how this needed to be enhanced in order to successfully grow the ridesharing community among known friends and also potentially to strangers. The prototyping approach is supported by interviews and group discussion. The initial rideshare prototype was designed to operate using a web browser, so that it could be accessed using any web-enabled phone, laptop and desktops, thus maximising the number of people who could participate in sharing using their own equipment. The prototype had a very limited functionality in that it only allowed people to send ride messages and information about seeking and offering rides. Even over a short four week trial of the first interface we observed a wide variety of practices and adoption, sharing and evolution of practices. In the beginning, most people sent formal ride messages by filling out form fields and few sent informal text messages because they were not revealed on the main page of the interface. However, once one participant realised that if no formal fields were filled out, only the informal text message would be revealed in the main page of the interface, the practice of informal messaging grew and it became the predominant form of communication. Collective information practice was at work.

5 Emerging security and privacy tensions in agile ridesharing

A number of emerging tensions between technical and cultural practices have been identified through collective information practice in our agile rideshare case study. These privacy and security tensions are listed in Table 1.

5.1 Precise tracking versus imprecision

While there are immense technical capabilities to track people's location, participants had concerns about who could see their location, even at fleeting moments. For example, providing journey start and end times would allow others to identify when they were away from their home and their car. Of particular concern was when both start and end of day rides, in opposite directions, were entered a day in advance, providing a clear understanding of when the participant would not be at home. However, a participant observed that even if return journeys were entered just once, then anyone with access to that data at any point in the future would find out a potentially ongoing commitment for the participant.

These concerns have been identified as real, and are similar to concerns raised in the mainstream media in Norway regarding the EU Data Retention Directive for data from mobile telephones which allows for tracing of the user [21,22].

The ability to be imprecise was valued for other reasons. Through use of the prototype we have observed that people often give only scant information as much as is sufficient to open a conversation. This allowed them to make a vague proposition to a broad audience and then to discuss specifics with a few people on a need to know basis. Further to practices that we can see developing in the field, matchmaking literature, such as by [16], offers lessons in obscuring or hiding the respective parties' personal information, while still providing relevant connections between appropriate parties, when technical assistance to do this is needed. But, most importantly, participants were able to control this information themselves in the doing, because the interface allowed such vagueness, by supporting free text messaging, rather than forcing specifics in formal fields.

The tension of providing data which helps an application to function, such as journey start times and locations, versus the need to obscure what is shown both immediately and when creating a total picture over time, is a tension which must be investigated in many social networking and sensor enabled applications.

5.2 Prior disclosure versus action over time

There is a tendency in technical systems to ask for prior disclosure of profile information from people with a view that other users want this information to make decisions about sharing. However, in direct conflict with this, many people do not wish to provide personal information about themselves, especially to strangers, and ideally not even to "potential ride sharers", but rather only to the person who is going to be in the car with them. The accuracy of profile information is anyway questionable. People are more likely to come to trust other people either through social connection, referral and reputation, or through their actions over time.

Another facet of this tension is the need to acquire information to allow for greater privacy and security. For example, some female participants stated they would only wish to ride with women. This is in keeping with the traditional practice that women can wait for other women to use rideshare across the East Bay of San Francisco bridge, a rideshare process which has been in place for 30 years [23]. Therefore, gender may be a reasonable question to ask potential rideshare participants. However, there was a strong reluctance by participants to enter gender and other information on the profile form, to the extent that we have now removed these questions from the profile form and provided a free text field instead (seen in Figure 1 below). This was seen as giving the users more control over what they chose to share.

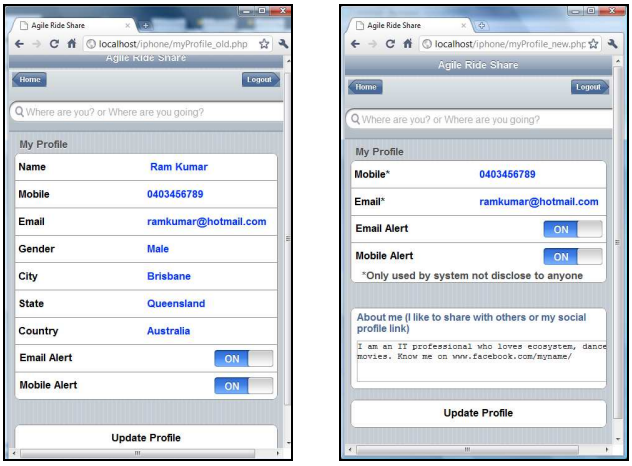

Figure 1: Original profile page (left) and current profile page (right)

Interestingly, although a key feature of agile ridesharing is the ability to bring unrelated people together, in the case of established groups, simply a recognisable nickname may be all that is required to fully detail a prospective journey. This introduced the human ethics consideration of "only collecting from the users the data required." Sometimes participants already know all details concerning gender, address, how to meet and what the vehicle looks like, and hence this data should not be compulsory to enter, since the system does not need to know this information, only the riders do. Thus we see again collective information practices at work.

5.3 Moderation versus referral and reputation

Moderators, people who would vet potential new participants and scrutinise the rides posted to ensure acceptability, were discussed with the participants and the idea was discarded due to there being too much responsibility placed on one person. Possible issues range from loss of life through to smaller offences such as pick pocketing or unsafe driving [23].

A participant used the example of a referral chain from her baby sitting circle. In this case, a circle member could recommend a new potential circle member, and the circle would make a decision. Having made the decision to include the new member, each participant chose who from the group they would let babysit their children, so there was another level of individual decision and control.

Referral chains may have a similar responsibility problem in much the same way as moderators, though the relationship is more direct and hence the risk is reduced. Instead of moderators and referral chains, allowing people to make their own groups gives individuals the greatest control [9].

Also discussed was the use of reputation systems [11]. While the agile ride share system makes strong use of social networking technologies on the internet, the people who are travelling together may be work colleagues, neighbours, or family members. Therefore, there were mixed feelings about reputation systems, in which the person travelled with is assessed and the score advertised on the rideshare system, although this does have potential as a method that reveals community trust built over time [9].

5.4 Underlying infrastructure versus accountability and transparency

At the lowest infrastructure level was the question, "Who has access to the database of user and ride information?" Attention was drawn to the concern that although the current interface protected the privacy of the individual, once the information was in the database a future design may make the information accessible. This led to questions of how to hide the information even from the designers, while allowing filtering and searching. Possible solutions, such as predicate cryptography (which allows users with the relevant attributes to view a message, while all other users may not), create a tension due to a lack of flexibility with future designs and the lack of control and visibility by the creators of the application.

A further tension exists with the expectation participants had that the service would be provided free of charge. For a prototype application with a small group of users, the design, development, maintenance, sending of SMSs to participants regarding rides, and connection and storage infrastructure costs may be included in a research budget. For a large application with millions of users, these costs would be considerable, and would typically be offset by either advertising with tracking cookies, or else by accumulating information about the participants and providing that information to interested parties, which may be the participants themselves (such as ride predictions for best times and places for rides). Both scenarios impact privacy.

Finally, the issue, common amongst social networking applications, was identified that it is difficult for users to view what others see about them. Further, there was the realisation that participants had no control over what other participants post. For example, even though participant *RLady* consciously makes a decision to never publish when she was not going to be home, another participant could write "Picking RLady up from her place at 10am." The above three concerns are indicative of tensions between individual or collective social practices that are accountable on a small scale and the implications of supporting these practices with an underlying technical infrastructure that has the capability to easily support large scale sharing of information.

6 Conclusion

We developed an agile ridesharing prototype mobile social software system and trialled it in order to explore the collective information practices that might be developed through its use in organising ridesharing. The paper contributes a practical example of designing for *collective information practice*, an approach proposed by Dourish and Anderson. A number of emerging security and privacy tensions between technical and cultural practices have been identified through examining the collective information practice in ridesharing. These tensions are: precise tracking versus imprecision; prior disclosure and setup versus action over time and in the moment; moderation versus referral and reputation; and underlying infrastructure versus accountability and transparency. A key aspect of design involves paying attention to people's practices and matching the system technical capability to these practices, so that technical capabilities support growth of collective information practice and do not introduce conflicts with human needs.

Acknowledgements

We gratefully acknowledge the contributions of our participants and reviewers.

References

1. Acquisti, A. and Grossklags, J., Privacy and rationality in individual decision making, Security & Privacy, IEEE (2005)
2. Bell, G. and Dourish, P., Yesterday's tomorrows: notes on ubiquitous computing's dominant vision, Personal and Ubiquitous Computing, Springer (2007)
3. Brereton, M. and Ghelawat, S. Designing for participation in local social ridesharing networks: grass roots prototyping of IT systems, PDC, ACM, 2010
4. Brereton, M., P. Roe, M. Foth, J. M. Bunker and L. Buys. Designing participation in agile ridesharing with mobile social software. OzCHI, ACM (2009)
5. Carlson, R.C., Anatomy of a systems failure: Dial-a-ride in Santa Clara County, California, Transportation, Springer, 1976
6. De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L. and Zurko, M. Adaptive Security Dialogs for Improved Security Behavior of Users, INTERACT, Springer (2009)
7. Dourish, P., and Anderson, K. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena, HCI, Lawrence Erlbaum Assoc. (2006)
8. Dourish, P., Grinter, B., Delgado de la Flor, J., Joseph, M.: Security in the wild: user strategies for managing security as an everyday, practical problem, PUC (2004)
9. Ghelawat, S., Radke, K. and Brereton, M., Interaction, privacy and profiling considerations in local mobile social software: a prototype agile ride share system, OzCHI, ACM, 2010
10. Heyer, C. and Brereton, M., Design from the everyday: continuously evolving, embedded exploratory prototypes, DIS2010, ACM (2010)
11. Josang, A. Ismail, R. and Boyd, C., A survey of trust and reputation systems for online service provision, Decision Support Systems, Elsevier (2007)
12. Lampe, C., Ellison, N., and Steinfield, C.A Face (book) in the crowd: Social searching vs. social browsing. Computer Supported Cooperative Work, ACM (2006)
13. Patil, S., and Lai, J. Who gets to know what when: configuring privacy permissions in an awareness application, SIGCHI, ACM (2005)
14. Sasse, M.A., Brostoff, S. and Weirich, D. Transforming the 'weakest link'- a human/computer interaction approach to usable and effective security, BT Tech Journal, vol 19, no. 3, 122-131 Springer (2001)
15. Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies, Security and Privacy, Citeseer (2007)
16. Shin, J.S. and Gligor, V.D., A new privacy-enhanced matchmaking protocol, NDSS, Citeseer (2007)
17. Shostack, A., and Stewart, A. The New School of Information Security. Addison-Wesley Professional, Upper Saddle River, N.J., 2008.
18. Sotirakopoulos, A., Hawkey, K. and Beznosov, K. "I did it because I trusted you": Challenges with the Study Environment Biasing Participant Behaviours, SOUPS (2010)
19. Spiekermann, S. and Grossklags, J. and Berendt, B. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, EC-2001, ACM (2001)
20. Star, S.L., The ethnography of infrastructure, American behavioral scientist, Sage Publications (1999)
21. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT
22. http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.
23. http://www.ridenow.org/carpool/#locations