Displaybook - Bringing online identity to situated displays

Abel Soares[1], Pedro Santos[1], Rui José[2]

[1]Mestrado em Informática, Universidade do Minho, Portugal
{pg13019, pg15964}@alunos.uminho.pt
[2]DSI, Universidade do Minho, Portugal
rui@dsi.uminho.pt

Abstract. This work is part of a study in which we aim to explore multiple bridges between on-line and off-line forms of socialisation by creating bi-directional connections between Facebook and situated social interactions. In this paper, we specifically describe a study on the use of public displays for the public presentation of data from the Facebook profiles of people near the display. The key challenge is how to map the concept of sharing information within a social network, to the concept of sharing information with the places you visit. For this to be viable, people must have full control over what they share and in what circumstances they will share it. This paper addresses this issue by studying the sharing alternatives, how this sharing of profile data in a public display is perceived by people and what are the main factors affecting that perception. The results suggest that, overall, people seem to be willing to expose parts of their Facebook profiles if given proper privacy controls. However, the study has also revealed a clear gap between privacy control in Facebook and the type of privacy controls that would be needed for this particular use of Facebook information.

1 Introduction

With their increasingly huge popularity, Social Network Sites (SNSs) have been reshaping many notions of socialisation. These sites are essentially about people wanting to stay connected with their friends and other people around them. This normally involves sharing with those people information regarding multiple facets of their lives. By feeding their social profile, posting content, expressing feedback and commenting on the activity of others, people are continuously generating massive quantities of user generated content that is quickly disseminated through the user network. All this activity is inherently on-line, occurring in the web almost as a parallel world of relationships and interactions that may seem independent from the situated interactions of the physical world. However, research has shown that Facebook connections normally have a strong correlation with off-line proximity [1][2]. More than a way to meet new people, SNSs are mainly a new mechanism for

managing already existing connections, albeit weak ones. Many of these "weak ties", i.e. relationships with people outside the normal groups of which we are a part of, emerge from the existence of a common offline element, such as working in the same place, studying at the same college, or frequenting the same places. The role of these weak ties in SNSs is well-know, but the role of SNSs in the off-line interactions between those people has been less explored, meaning that there is still a strong potential in extending SNSs to situated interaction and presence. This might be particularly important to the process of meeting new people, something that SNSs still do not seem to afford very effectively [2].

1.1 Bridging between on-line and off-line social interactions

This work is part of a study in which we aim to explore multiple bridges between on-line and off-line forms of socialisation by creating bi-directional connections between SNSs and the situated social interactions occurring between sets of co-located people. In this paper, we specifically describe a study on the privacy implications for the use of public displays to present data from the Facebook profiles of people near the display.

The motivation behind this work is the idea that, in some situations, bringing SNSs profiles into the off-line world of situated interactions may enrich those interactions. SNSs profiles may provide a relevant, yet spontaneous and informal, representation of identity that can be useful for many types of situated services. Public displays, in particular, may provide an additional channel for self-exposure and new opportunities for augmenting co-located social interactions. Also, from the perspective of SNSs, this type of bridge may lead to a stronger presence in the life of their users, something that may turn out to be crucial to their long-term sustainability.

However, the use of Facebook profiles outside their normal context also raises considerable challenges, both technical and social. The key challenge is clearly how to map the concept of sharing information within a social network, to the concept of sharing information with the places you visit. For this to be viable, people must have full control over what they share and in what circumstances they will share it. This paper addresses this issue by studying the sharing alternatives, how this sharing of profile data in a public display is perceived by people and what are the main factors affecting that perception.

To support this study we have developed Displaybook, an application that enables people to share Facebook profile information with public displays. The information from a particular profile is only presented when that person is detected near a display. This achieved by associating a Bluetooth address with each profile and scanning Bluetooth devices in the vicinity of the display. When installing the application,

people are given the opportunity to choose between a set of privacy preferences. We have collected data on the privacy specifications selected by people and we have conducted interviews with some of the users to gain a more in-depth perspective on individual perceptions. The results suggest that overall people seem to be willing to expose parts of their Facebook profiles given proper privacy controls. However, the study has also revealed a clear gap between privacy control in Facebook and the type of privacy controls that would be needed for this particular use of Facebook information.

2 Related Work

The use of SNSs within multiples situations of everyday life is increasingly possible through all forms of mobile versions of the respective software, allowing people to continuously maintain their on-line presence and possibly generate life streams representing their off-line social activity. However, these mobile applications do not really take advantage of the opportunity to connect the social context of SNSs with the social context of co-located people interacting with each other.

One of the early experiments in bridging between social networks and social situations, more specifically a conference setting, was proposed by Konomi et. al. in [3]. The conference badges were RFID tags and when participants approached a display, a social network was presented base on publication records in DBLP. The expectation was that presenting the professional social network within that specific context would help co-located participants to communicate and develop relationships.

The injection of real-world presence data into social networks is explored in CenceMe [4]. A mobile application is continuously collecting data from any sensors the mobile phone might have and inferring the current activity of the person. This data can then be injected into multiple social networks, including Facebook, thus enriching the information flow from the real-world to the SNSs. CenceMe also leverages on the social networks for defining access policies. It basically takes the buddy lists users have already created in those services to determine who can have access to the CenceMe data.

Kostakos has conducted a study in which Facebook connections of 2602 individuals were analysed in conjunction with data about their Bluetooth encounters [2]. This study provides important insight into the multiple similarities and shared connections between these two types of social structures. This work also involves the use of a Facebook application and Bluetooth, but in this case they are being used as data collection tools for studying the social networks themselves. In a separate piece of work within CityWare, Kostakos and O'Neill have also explored the use of a

Facebook application in association with Bluetooth traces [5]. In this case, Bluetooth mobility traces were presented in public displays, but the system also allowed people with the Facebook application to have access to data about their physical co-presence with members of their social network.

WhozThat [6] uses the SNSs profiles of people nearby to create context information that can then be used to support spontaneous interactions or drive the music selection. People are expected to use a mobile phone running an identity sharing protocol that will advertise their on-line identities to the other nearby devices. This system does not consider the use of public displays or any explicit selection of which information to share, but it is an example of using SNSs profiles as a sort of personal data aura that can be used to mediate digital self-exposure.

Bohmer and Muller [7] conducted a study on the exhibition of SNSs profiles in public settings. Using mockup images they asked people about their willingness to expose profile information in two types of what they called social signs. The first was a personal social sign projected around the person and showing parts of the respective profile. The second was a interpersonal sign, projected in such a way to link two people and representing some type of connection between them, such as having a mutual friend or sharing an interest. The study consisted in presenting the scenarios and interviewing people about their perception of those hypothetical uses. The results suggested that there is some interest in the overall idea, but also highlighted serious concerns about the particular circumstances in which such exposure should occur. This study, however, did not address real usage situations or how to map particular types of self-exposure to specific situations.

3 System Overview

3.1 Mapping Facebook concepts into public displays

A key part of this work is to study how to map Facebook concepts to the needs of publication in information displays. Regarding which information to take from Facebook, we have studied the existing information and how it can be accessed. In principle, any piece of information and activity generated by a Facebook Profile could be shown on the public display, as long as the respective user had authorised access to that information to our Displaybook application. However, information presentation in public displays represents a very unique context for exposing personal information. Therefore, individuals should have a clear opportunity to specifically express permissions to that particular form of presentation. We have focused specifically on profile information, making a separation between public information (name and photo) and non-public information (Likes, music, TV, movies, books, quotes, About

me, Activities, Interests, Groups, Events, Notes, Birthday, Religious and political views, Education History, Work history and Facebook status).

The information sharing model in Facebook was conceived with a rather different set of assumptions, and thus it was without surprise that we have identified a number of mismatches when trying to map that model into a model for presenting data in public displays. More specifically, the following issues were identified:

- Facebook privacy model defines how information in Facebook can be accessed, in this case by applications. It does not really support any type of considerations on how the information is going to be used. This basically means that before we present users with our own application-specific privacy settings, they will first have to go through the standard privacy settings in the Facebook platform, where they will have to authorise information access regardless of how it will be used by Displaybook.
- Facebook applications are mainly designed to be used interactively, and thus the basic permission model only allows applications to access user's data when the user is logged in. There is an alternative to overcome this limitation in which users may allow applications to access their data without the need of an active session. This is however not a common need for most Facebook applications and represents an additional step for privacy-sensitive users.
- The user can easily specify its privacy preferences for an application, but it is normally very easy for an application acting on behalf of the user to gather data about friends of users (and friends of friends), even if they are not aware of this information usage. This is a reflection of the Facebook network and privacy model, in which friends normally have the ability to access much more data than "anyone".

To summarize, and because of these mismatches, simply installing Displaybook seems to entail many more privacy risks than what it would seem necessary when we consider the information actually presented on the public displays. Regardless of the information actually being presented, regardless of any blurring or aggregation mechanisms that might be used to preserve privacy, the fact remains that to be usable, Displaybook will always end-up having considerably extensive permissions to access Facebook profiles.

3.2 The Displaybook application

As part of this study, we have developed the Displaybook application for enabling the presentation of parts of Facebook profiles in public displays. The application is composed by 4 key components, as represented in Fig. 1.

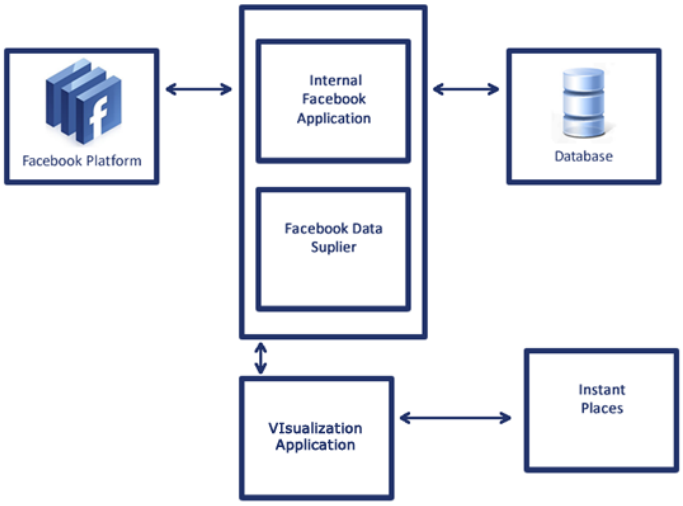

Fig. 1. – System overview.

Internal Facebook Application – This is an application that runs as a Facebook application and can be accessed from inside Facebook. It serves as an integration point for users, allowing them to specify privacy settings for data on displays and associate their Bluetooth MAC address. Users of our system must necessarily take the step of installing this application from their Facebook account.

Facebook Data Supplier – This is a web application that uses the Facebook API to retrieve the necessary data about the profiles that are using Displaybook. The data supplier will receive a set of MAC addresses (currently detected in the place) and will get all the Facebook data associated, keeping in mind the permissions that users have set.

Visualization application – This application supports two types of Flash-based visualizations of the Facebook profile data. The first visualization, represented in Fig. 2, displays the list of present profiles. Each profile is represented by an icon that may include the name and the photo, unless the user has denied any of this information. The second visualization, represented in Fig. 3, displays an aggregate view of the information from the multiple users detected in the place. This information may include gender, birthday, location, relationship status, hometown, education and high school education and is presented without being associated with any particular profile. When data is similar for users, the tag gets more relevance, with a superior size compared to others.

Fig. 2. – Profile visualization application.

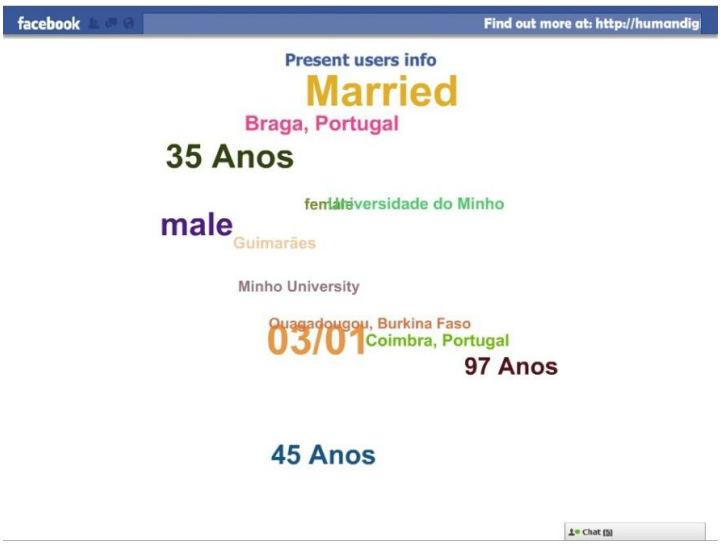

Fig. 3. – Aggregate visualization application.

Instant Places – Instant Places is a Bluetooth based sensing platform and provides information about open Bluetooth presence sessions. A session symbolizes a presence of a Bluetooth enabled device in the place. This information is obtained from routers running Bluetooth scanning software.

When the system is running, the visualization application queries Instant Places and obtains a list of the Bluetooth devices that are currently present near the display. The application will then query the Facebook data supplier for data associated with those Macs. The Data Supplier will find correspondent Facebook Profiles IDs and their permissions settings in our database and use Facebook Platform API's to access data about the users. After that, the Data Supplier will filter all data according to each user permission setting and respond back with the data to the Visualization Application in XML format.

3.3 Setting privacy policies with Displaybook

When a user first goes to the Displaybook application, he or she must go through a set of dialogs for setting privacy preferences. The first dialog is meant to give Displaybook permission to access the public profile data. This is a common procedure when someone uses a Facebook application and is absolutely necessary for the system to be able to present parts of the profile.

Fig. 4. – Request for permission dialog.

Immediately after, the user will be asked to give offline access and permission to some of his or her profile information. This will make possible for Displaybook to

retrieve Facebook Profiles information on behalf of the user. It also indicates the profiles categories that the system may ask for, such as Birthday and Education, Hometown and Location, and Relationship Status. This is a generic permission from Facebook. Users will later be asked within the application to refine exactly which information they want to display.

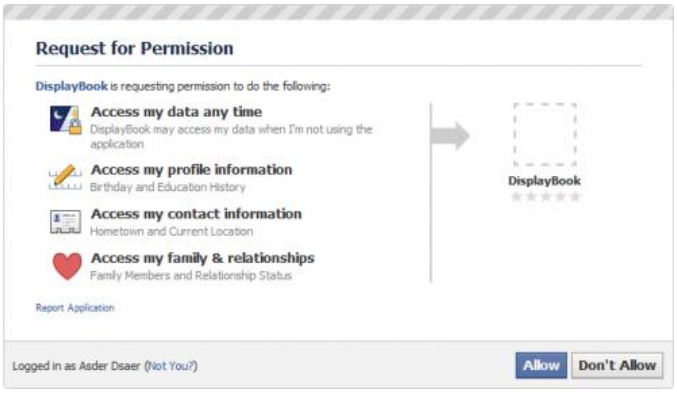

Fig. 5. – Extended Permissions Dialog.

In the next step, people are asked to submit their mobile device Mac address. This will later be used to enable the displays to recognize the presence of the user.

Fig. 6. – MAC address association.

Now that Displaybook already has access to the Facebook information, the permissions dialog can be used to configure exactly which profile data users have interest in showing on the displays. The answers to this dialog were an important part of our study.

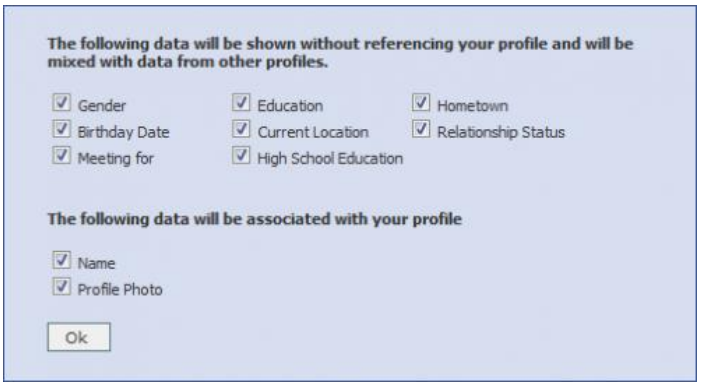

Fig. 7. – Permissions Manager.

4 Evaluation

4.1 Deployment

We have used two public displays in our department as the basis for the deployment. This is a place closely linked with a particular community, the Department staff and students. Many of them share Facebook connections, and most people could easily be informed about the system and invited to join in.

The content generated is a simple web-based application. The respective URL is given to the display software, which will show that content whenever requested. Bluetooth sensing is in place to support the presence recognition and also to support explicit interaction using a simple command language for the Bluetooth Names.

The announcement of the applications was made by sending an e-mail to the local e-mail lists and through Facebook itself. The announcement included an indication of where to install the Facebook application, the privacy policy and usage information, especially how to create the connection between Bluetooth Mac addresses and the identity profile.

4.2 Results

There were nine users using Displaybook during the one week long evaluation period. They were all part of the Department community, including academic staff, researchers and administrative staff. Eight of them have used the privacy manager to change their data permission settings. The data collected on how they set their privacy settings can be summarized as follows:

- **Name:** No one has changed permissions for name. It was always available, for all users, through the time the experience occurred.
- **Profile photo:** Three persons have removed permissions to show the photo. Two of them have done so when first confronted with the privacy dialog, and one after having seen her photo on the display.
- **Education:** Two persons have removed permissions to show education data. One initially, one after a while.
- **Birthday:** Three persons have denied presentation of their birthday.
- **Relationship Status:** Five persons have blocked permissions to show their relationship status.
- **Location:** Everyone has allowed presentation of their location (Home Town)

Users who have blocked the availability of the profile photo on the public displays, have also expressed that they don't really feel comfortable about having their identity displayed in public spaces. One user has reported having an unpleasant experience when people recognize him and approached him to talk about it. This kind of confrontation does not exist in a virtual presence and clearly shows the type of conflict that may occur between what people feel and construct about their virtual existence, and what happens when that same virtual identity suddenly gains a situated existence in physical space. This particular example, and also some of answers in the interviews, have shown that names and photos were seen as particularly sensitive information when presented in this context. This reveals a clear contradiction between what Facebook regards as public data in an online environment (name and photo) and what people would be more willing to show on a public display.

4.3 Lessons Learned

One of the lessons from this work has been to feel as developers the extent of what it means to say that Facebook is an evolving reality. If considering that this work has been conducted within a three months period, we still had to face changes in the underlying API, in the application naming policies, in the concept of "fan page" (now a Facebook page liked by people), and most importantly multiples changes in the privacy policies and controls. More than presenting these problems as complaints, we expected to highlight how important it might be for Facebook developers to reduce their exposition to changes in the Facebook API or even in the application and privacy policies.

The way we had to present the privacy settings has revealed a clear mismatch between Facebook assumptions on the use of profile information and our own use of that information. Facebook assumes that either information is shared or is not shared, which is probably a reasonable assumption within the normal Facebook setting. However, within the setting of our study, it was clear from the beginning that the way in which information was presented and even the circumstances surrounding its

presentation would be important elements in how people perceive that their privacy is being affected.

5 Conclusions

The use of Facebook for creating user-generated content on public displays clearly holds a lot of potential. However, control by users is crucial in such approach, and this work has clearly shown how Facebook privacy policies are not aligned with this particular usage of Facebook data. When bringing Facebook Profiles into public displays, privacy concerns enter a new dimension that is not necessarily the dimension exposed in web environments, where typically social platforms exist. The identification of users is a concern in public spaces, something that is normally not a major issue in SNS. As future work, we intend to study how privacy policies for self-exposure in public displays can be expressed more effectively by users, and also how users can take more advantage of these features as a mechanism for situated interaction.

References

[1] N. Ellison, C. Steinfield, e C. Lampe, "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites.," *Journal of Computer-Mediated Communication*, vol. 4, 2007.

[2] V. Kostakos, "An empirical study of spatial and transpatial social networks using Bluetooth and Facebook," *0910.4292*, Out. 2009.

[3] S. Konomi, S. Inoue, T. Kobayashi, M. Tsuchida, e M. Kitsuregawa, "Supporting Colocated Interactions Using RFID and Social Network Displays," *IEEE Pervasive Computing*, vol. 5, 2006, pp. 48-56.

[4] A.T. Campbell, S.B. Eisenman, K. Fodor, N.D. Lane, H. Lu, E. Miluzzo, M. Musolesi, R.A. Peterson, e X. Zheng, "CenceMe: Injecting Sensing Presence into Social Network Applications using Mobile Phones (Demo Abstract)."

[5] V. Kostakos e E. O'Neill, "Capturing and visualising Bluetooth encounters.," *CHI 2008, workshop on Social Data Analysis*, Florence, Italy.: 2008.

[6] A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, e R. Han, "WhozThat? Evolving an ecosystem for context-aware mobile social networks," *Network, IEEE*, vol. 22, Jul. 2008, pp. 55, 50.

[7] Matthias Böhmer e Jörg Müller, "Users' Opinions on Public Displays that Aim to Increase Social Cohesion," *Proceedings of The 6th International Conference on Intelligent Environments. Kuala Lumpur 2010, Malaysia; to appear.*