Privacy Settings for Smart Phone Applications Post-Installation

Ashley Anderson University of North Carolina Charlotte- HCI Lab
9201 University City Blvd
Charlotte, NC 28223
anander@g.clemson.edu

ABSTRACT
The number of smart phone applications on the market is growing daily. These applications are written by third party developers and can access personal data on a user's phone. This leads to security concerns because of the current privacy mechanisms. It is either all or nothing, since one has to approve all permissions to even install the application. We have implemented an interface to be placed over existing applications that allows the user to authorize permissions as they use the application. This will allow for users to be able to interact with the application without leaving their data completely open for sharing. We intend for our interface to improve the mental model of data sharing on smart phone as well as the memorability of what data is shared by which applications. In this paper we will introduce our interface prototype and show the results of interview questions asked to subjects who used our system.

Keywords
Human-Computer Interaction, Smart Phone, Privacy, Applications

1. INTRODUCTION
The number of smart phone applications on the market is growing daily. An application is a program or process that runs on the smart phone's operating system, and people use them for convenience and entertainment purposes. The security concerns that arise from installing and using these applications are also on the rise. These involve lack of information about what the data is being used for and why, as well as increased access to device hardware. This is because of the privacy system that is currently in place.

We propose a privacy settings interface to be placed over existing applications. Using this interface, the user authorizes permissions as they use the application. Users are able to interact with the application without leaving their data completely open for sharing. We intend for our interface to improve the mental model of data sharing on smart phone as well as the memorability of what data is shared by which applications. Our interface, applications, study methodology and the results of our study will be detailed in this paper.

Our prototype is tested on two applications of different contexts. The first application is a game with an added profile screen. The other is a journal application where the user can save a journal entry with a picture or a voice clip. We tested these application on subjects, then asked them a few questions about their experience in an interview format. We then analyzed their responses and drew conclusions about their mental model of privacy, memorability of what they shared, and the degree of ease of use of our interface.

2. MOTIVATION AND BACKGROUND
There are a few problems that we noticed, and prior research, that became the motivation for this project. The first of these problems is the skewed mental model of privacy, or lack of one, that the majority of people have about social media websites such as Facebook [1]. Research shows that people in general have no idea what information they are actually sharing about themselves or what the privacy settings do [1]. This leads to users making decisions they may not be comfortable with. Furthermore, smart phones offer a similar platform for applications that access personal data. We believe that this lack of awareness extends to this platform as well.

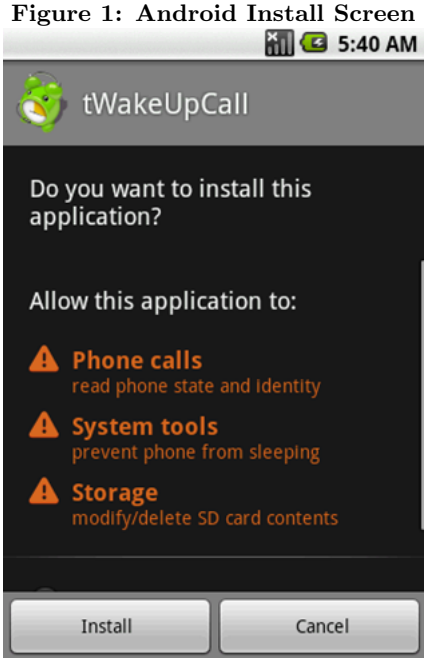
There is research attempting to improve privacy setting interfaces. For example, researchers developed AudienceView, a privacy feature for Facebook that lets one see their profile as a friend, a friend of a friend or a stranger which leads to a better mental model of what info is showing to whom [3]. Another example is the Expanded Grid. This interface presented privacy settings in grid format with data on one axis and people on the other. This interface provides users a general, compact view of all their settings [2]. However, all of the privacy settings interfaces explained here are separated from the context that they apply to.

To understand fully what the goals of our project are, we need to first understand what privacy really is. We are interested in data privacy, or designing such that the identity of any individual or entity contained in data cannot be recognized while the data remain practically useful [5]. Here we are designing for the smart phone specifically. Although we have implemented applications for the Android SDK, our in-

terface and the idea behind it can be extended to any smart phone operating system that supports applications [6].

Currently on the Android, when a user downloads an application from the marketplace they are met with a screen that shows a list of all data items and hardware it needs to access (Figure 1).

Figure 1: Android Install Screen



The user has to confirm these permissions before they can even install the application. It gives no information about what the data will be used for in the application and why. Our interface will change this by integrating the authorizations into the application itself, bypassing this screen altogether.

3. PRIVACY INTERFACE

Overall, our goals for the interface are to give users a better mental model of their privacy settings as well as increase memorability of what data items are being accessed and shared. The privacy interface consists of blue lock icons positioned next to the features they relate to (Figure 2). By locating the privacy icon adjacent to the data item it relates to, we provide a way for the user to make a connection between that feature of the application and the privacy setting. The icons are small and meant to be noticeable, yet unobtrusive. It is also designed to be basic, understandable and easy to use. If a user clicks on this icon, or on one of the feature buttons before authorizing the setting, a dialog box appears containing a toggle button, a description of what access the user is authorizing, and a button to save the setting(Figure 3)

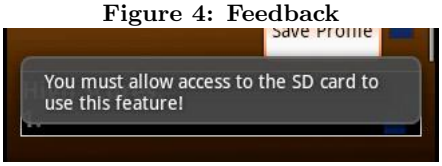
Initially all data access is turned off, so the user can authorize only some features of the application while denying others. Once a piece of data is authorized for the application to use, the user will never see this dialog again unless they wish to turn access off.

Figure 2: Data Item and Privacy Icon

Figure 3: Privacy Dialog Box

To do that, they click on the blue lock icon that has changed to the unlock position, which will reopen the dialog and allow them to change and save the setting again. However, they can still use parts of the application that do not require access at any time. If the user tries to use a feature but does not allow the application to access that data item, a feedback message will appear reminding them that they need to allow access to use that part of the application(Figure 4)

Figure 4: Feedback



4. IMPLEMENTATION

In order to test this interface we have to add it to applications a user can interact with. The first application called *Divide and Conquer*, was modified from an open source application provided by Google. It is a game where players divide the screen with a line while trying to avoid bouncing balls. We added a profile screen to this game so we could add features to attach our privacy interface onto(Figure 5). This profile screen includes email account, photo, about me, and high score data objects. The privacy settings needed to access the data items in this application are access to phone account, photo album, and the internet.

The second application, based on a diary, is completely original. It is called *Life Journal* and consists of a main screen where users navigate to the two other screens as well as look at a list of previous saved entries(Figure 6). On these two other screens users can create journal entries featuring either a picture taken from the camera or a voice clip sound recording. They also can tag a contact, which requires access to the contacts list and their current location, which requires access to the GPS. When the user saves an entry, it is stored in a database to be retrieved later on the main screen.

5. STUDY METHODOLOGY

The study is broken down into two phases, an interview phase and a deployment phase. Our goals are to get feedback on the usability of our model, what perceptions users

Figure 5: Divide and Conquer Profile Screen

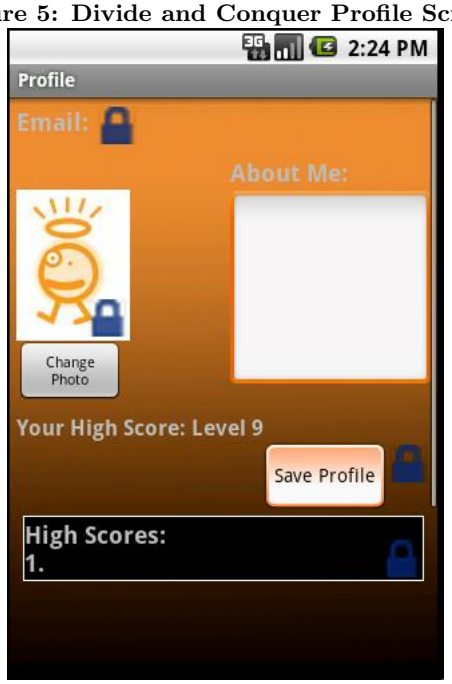
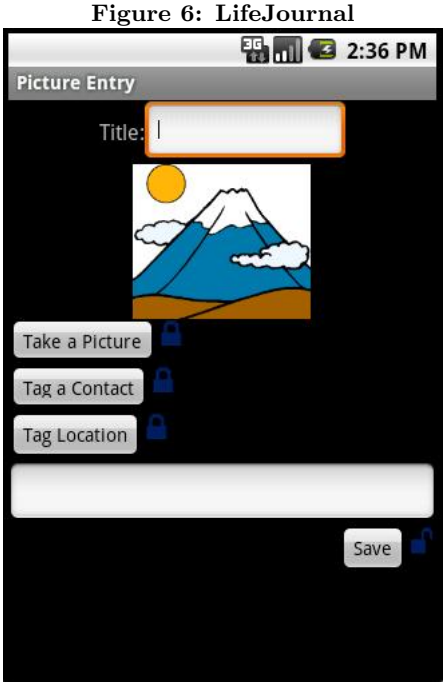


Figure 6: LifeJournal



have about privacy while using our model, and what do they remember about the data items being shared by the applications.

5.1 Interview

We started with an interview study. At the beginning of the session, the interviewer explains briefly about the privacy interface and our applications. They set up the phone and screen capture recording on the laptop for the test. The screen capture application records what decisions that the user makes while interacting with the privacy settings.

The subject is handed the phone and a sheet detailing three tasks for them to perform inside of our application, such as creating a profile, creating an audio journal entry and creating a photo journal entry. There are three of these tasks and they are designed to only last for three to five minutes total. Users can ask questions and make comments during this time because the audio is being recorded.

After this, the user is interviewed about their experience interacting with the applications and the interface. Some of the questions asked include the following:

- What data was allowed to be accessed? - How comfortable were you using this application? - What was your initial impression of interacting with applications this way? - Would you like to see privacy settings like this on more applications in the future.

Finally, the subject fills out a survey about their demographics and how they fit into the Westin privacy types. The Westin survey classifies a person's attitude toward privacy as Fundamentalist, Pragmatist or Unconcerned. A Fundamentalist does not like to share any of their data, a Pragmatist will exchange sharing of some data items with benefits, and someone who is Unconcerned doesn't care about where their data goes or how it is used [4].

5.2 Deployment

The deployment phase will be a longer term study that will test fully the user's memorability. We have not reached this phase yet in the study because we need to further improve and implement more features into our applications, so this is planned in the future.

All participants that are applicable will take our applications home with them after installing them onto their phone for a total of two weeks. Every few days we will send out reminders via our logging service telling the subjects to use our experimental applications for a few minutes each day. They will be asked to use the applications for two to three minutes, which will result in them having to interact with the privacy settings.

At the end of the two weeks, participants will be asked to fill out an online survey asking questions about their mental model and their experience using the applications.

6. RESULTS

Thus far we have interviewed 5 people. They were ages 20 to 25 with 3 females and 2 males. We gained important feedback enforcing that our ideas were well founded and that some aspects of our interface need to be improved on. We can also use this feedback to improve our study organization in the future.

Here are some quotes of positive feedback from some of our subjects

Subject 2:

It felt very secure. I was very aware of what access the applications had to data and it wasn't just a big "OK" button.

The subject was aware of what data the application was accessing, showing that he has some mental model of privacy after using the interface. Also, on a positive note our model made him feel secure as he was using the applications.

Subject 5:

Everything seemed pretty intuitive.

An intuitive interface is our goal, so this feedback lets us know that we are headed in the right direction. It may not be perfect, but we are getting there.

Some of our subjects offered suggestions for improving our model. For instance, some users felt that our original dialog was confusing. It contained an "OK" and "Cancel" button on the bottom instead of a "Save" button. When users clicked "OK" they weren't sure if they had actually changed anything. When it was changed it became clearer what was actually happening.

Subject 4:

I could find my way around it, but I had to ask some questions.

When they first encountered the interface, some subjects became confused about whether they were allowing or disallowing access with the toggle button. After asking a question and being given a short explanation of the interface, they realized what was happening and could understand how to use it. This means that we need to provide more information initially or make the interface even more understandable.

Subject 5:

Might not even need a save button. Could save just by toggling it on and off.

This subject suggested that a save button might not even be necessary for the privacy dialog. This is a valid suggestion and will be taken into consideration in future work.

7. CONCLUSION

So now we find ourselves asking, so what? What is the societal importance of this research? Society as a whole will benefit from this project by being able to have greater control over their personal data and privacy while still being able to use whichever cellular device applications they desire. Privacy will become more detailed than simply sharing everything or sharing nothing. Also, users will have increased control over what data items are shared when they are using applications on their devices.

The results so far show positive feedback on the new model as well as suggestions for continually improving the interface. Users expressed that it was fairly easy to use and made them feel more secure. In the future, we will continue to update the interface and move onto large scale testing.

8. ACKNOWLEDGMENTS

Thank you to Dr. Heather Lipford, Andrew Besmer, UNCC, and DREU for funding and support this summer.

9. REFERENCES

1. A. Besmer H. Lipford. Users' (Mis) Conceptions of Social Applications. In Proceedings of Graphics Interface, May 2010

2. H. Lipford, J. Watson, M. Whitney, K. Froiland, R.W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proceedings of ACM CHI 2010, April 2010.

3. J. Watson, M. Whitney, H. Lipford. Configuring Audience-Oriented Privacy Policies. In Proceedings of Workshop on Assurable Usable Security Configuration (SafeConfig), November 2009.

4. P. Kumaraguru, L. Connor. Privacy Indexes: A Survey of Westin's Studies. CMU-ISRI-5-138, December 2005.

5. L. Sweeny. Computational Disclosure Control - A Primer on Data Privacy Protection. Massachusetts Institute of Technology, 2001.

6. Android Developers. http://developer.android.com/index.html, 2009.