THE ILLUSION OF PRIVACY CONTROL
THE CASE OF THIRD-PARTY APPS ON FACEBOOK

A Thesis in
Information Sciences and Technology

by
Na Wang

© 2011 Na Wang

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

December 2011
The thesis of Na Wang was reviewed and approved* by the following:

Heng Xu
Assistant Professor of Information Sciences and Technology
Thesis Advisor

Mary Beth Rosson
Professor of Information Sciences and Technology
Director of Graduate Programs

Jens Grossklags
Assistant Professor of Information Sciences and Technology

*Signatures are on file in the Graduate School
ABSTRACT

The extensive display of personally information by users of Facebook has made privacy concerns particularly salient. Many of the most popular third-party applications (apps) on Facebook have been transmitting users’ personal information to dozens of advertising and Internet tracking companies. At the same time, despite the presence of some privacy norms, there are relatively few well-established institutional rules and practices governing online social networks, which give rise to opportunism. The main objective of this work is to address the need for a paradigm shift in understanding and addressing users' privacy risks in the context of online social network with a specific focus on the third-party apps. Toward this end, we collected data from 1800 most popular apps to figure out what kinds of personal information these apps were trying to obtain from users and their friends. In addition, we developed our own Facebook application and conducted a series of experiments to observe third-party apps' practices for privacy notice and consent. Our analysis reveals that: 1) there is a large amount of users' personal information transmitting from Facebook to third-party apps, 2) users’ current privacy settings on Facebook can be violated by third-party apps, and 3) the current authentication dialog for privacy notice and consent is ineffective in terms of reflecting the third-party apps' information practices.

To address these problems, we propose two new interfaces for the third-party app’s authentication dialog to: 1) empower user control to limit apps' data access and restrict apps' publishing ability during the process of adding the apps to their profiles, and 2) alert users when their global privacy settings on Facebook are violated by the apps.
user study was conducted to evaluate the authentication dialogs we proposed. In sum, our research suggests that current privacy control settings on Facebook can be violated by third-party apps. Further research is expected to design and enforce stronger privacy control without violating user privacy settings. In addition, the authentication dialogs for privacy notice and consent should be designed to provide transparency to users in terms of the third-party app's information accessing and publishing abilities. Using the groundwork laid down in this study, future research along various possible directions could contribute significantly to extending our theoretical understanding and practical ability to empower users with privacy control on Facebook and other online social networks.
# TABLE OF CONTENTS

LIST OF FIGURES ............................................................................................................. vii
LIST OF TABLES ................................................................................................................ viii
ACKNOWLEDGEMENTS ................................................................................................. ix
Chapter 1 Introduction ................................................................................................. 1
Chapter 2 Related Work ............................................................................................... 4
Chapter 3 Overview of Users’ Information Control on Facebook .............................. 6
  Users’ Information Control on Facebook ................................................................. 6
  Information Control Between Facebook Users and Third-Party Apps .................. 7
  User Interface ............................................................................................................. 8
  Data Permissions Defined in Developers’ Source Codes versus Shown in User
  Interface ..................................................................................................................... 9
  Graph API .................................................................................................................. 13
Chapter 4 Overview of Facebook Third-party Apps ................................................. 15
Chapter 5 Third-party Apps’ Practices for Privacy Notice and Consent .................. 19
  A display test ........................................................................................................... 20
  A limitation test ....................................................................................................... 21
  A privacy violation test ............................................................................................ 21
  A reflection test ........................................................................................................ 23
Chapter 6 Proposed Designs ....................................................................................... 27
  Problems with the current authentication dialog (AD) ............................................ 27
    Problem 1 ............................................................................................................... 27
    Problem 2 .............................................................................................................. 28
    Problem 3 .............................................................................................................. 28
  Design Principles .................................................................................................... 29
    Principle 1 ............................................................................................................. 30
    Principle 2 ............................................................................................................. 30
    Principle 3 ............................................................................................................. 30
    Principle 4 ............................................................................................................. 31
  Alternative Authentication Dialogs ......................................................................... 31
    Monochrome authentication dialog (MONO) ....................................................... 34
    Polychrome authentication dialog (POLY) ........................................................ 35
Chapter 7 User Evaluation ........................................................................................... 36
Participants ................................................................................................................................. 36
Questionnaires ............................................................................................................................... 36
Discussion ....................................................................................................................................... 38
  “In the Right Direction” ............................................................................................................... 38
  Friends’ information ..................................................................................................................... 39
  Comparing Different Authentication Dialog Designs ................................................................. 40
  Overall likability ............................................................................................................................ 43
Chapter 8 Conclusions and Future Work ....................................................................................... 44
  Future work .................................................................................................................................. 46
Bibliography ..................................................................................................................................... 48
LIST OF FIGURES

Figure 3-1. User Interface of Privacy Settings on Facebook.........................................................6
Figure 3-2. The OAuth 2.0 protocol. ..................................................................................................7
Figure 3-3. Interface Associated with the Application Authentication............................................9
Figure 3-4. Post-Installation Privacy Settings for Third-Party Apps. .......................................13
Figure 4-1. Users’ Personal Information Accessed by Third-Party Applications. .................17
Figure 5-1. Screenshot of a Facebook Application Requesting Access to User’s Photos and Videos and Friends’ Photos and Videos.................................................................20
Figure 5-2. The Process of The App Discloser User’s Private Information. .............................23
Figure 5-3. The Application’s Authentication Dialog with Extended Permission “user_photos”.................................................................................................................................25
Figure 5-4. The Real Amount of Information Could Be Released by Extended Permission “user_photos”..................................................................................................................25
Figure 6-1. Screenshot of The Authentication Dialog Showing Different Types of Permissions. ........................................................................................................................................28
Figure 6-2. A New Monochrome Interface Design for Facebook Third-Party Authentication. ...............................................................................................................................34
Figure 6-3. A New Polychrome Interface Design for Facebook Third-Party Authentication........................................................................................................................................35
LIST OF TABLES

Table 3-1. Contents of Publishing Permissions: Developer View versus User View .... 10

Table 3-2. Contents of Data Permissions for Users: Developer View versus User View .............................................................................................................................. 11

Table 3-3. Contents of Data Permissions for Users’ Friends’ Information: Developer View versus User View ........................................................................................................... 12

Table 4-1. Users’ Information Releasing Description................................................................................................................................. 16

Table 4-2. Summary of Different Type of Applications and Their Information Requests......................................................................................................................... 18

Table 6-1. The Design Elements ................................................................................................................................. 33

Table 7-1. Comparing Authentication Dialogs ......................................................................................................................... 40
ACKNOWLEDGEMENTS

It is a pleasure to thank the many people who made this thesis possible.

I would like to thank my advisor Dr. Heng Xu. I am deeply grateful to Heng for giving me the chance to explore my research interests and the guidance to avoid getting lost in my exploration. Heng is the best advisor and teacher I could have wished for.

I also thank Dr. Jens Grossklags. Jens is sharp, cheery, perceptive, and mindful of the things that truly matter. I thank him for all his advice and support.

I would also like to thank my friends in State College, Yu Zhang and Yan Cao. They ensured I was constantly engaged and entertained along the way. Among many other things, Yu gave me thoughtful and detailed feedback on this thesis.

Finally, I would like to thank my family, especially my parents, for their absolute confidence in me.
Chapter 1

Introduction

Facebook has transformed from a localized college network website to one of the most popular social networking sites in the world with 500 million active users from more than 180 countries. Altogether, these users spend over 700 billion minutes per month on Facebook ("Facebook Statistics," 2010).

Facebook allows and encourages user to share content on this platform. An average Facebook user creates 90 pieces of content each month (including web links, news stories, blog posts, notes, photo albums, etc.). Taken together with a great number of other documents that users interact with (e.g., pages, groups, events and community pages totaling 900 million objects), Facebook gradually expands into a ubiquitous giant content repository ("Facebook Statistics," 2010).

As social networking users are potential consumers, more and more businesses begin to exploit Facebook for commercial benefits. First, social networking sites can act as promotional platforms. In addition to paying for traditional advertisements, companies frequently create profile pages and utilize those to foster brand awareness and to publicize their products, services, or events with their fans. Second, businesses and other developers are finding more direct ways to interact with consumers and to generate and accumulate revenues. Social applications written by third parties are a particularly quickly growing source of business revenues and consumer access. For example, Facebook users undertake 20 million individual installations of the available social applications every day ("Facebook Statistics," 2010).
Social networking sites and third-party applications developers have a subtle relationship. On one hand, the third-party applications enhance the attractiveness of the networking platform and increase their revenues through profit sharing; on the other hand, the direct participations of third parties pose significant privacy risks for users and introduce challenges concerning the effective management of consumer expectations and preferences as evidenced by previous privacy breach events. For example, in a recent article by the Wall Street Journal, it was reported that many popular entries of the 550,000 Facebook applications have been transmitting identifying information about users and their friends to dozens of advertising and Internet tracking companies (Steel & Fowler, 2010).

Most third-party apps utilize Facebook application programming interfaces (APIs) to access user data. Although Facebook offers privacy settings to users and let them to restrict the accessibility of their information, these privacy settings are mostly designed for limiting the data sharing among users. When the scope of data sharing extends to the scale between users and third-party apps, the situation becomes more complicated and users’ privacy control options on Facebook become problematic. Thus, it is important for us to investigate this social platform of data sharing between users and third-party applications (apps) on Facebook and to examine the extent to which potential privacy breach may exist in this context.

The main objective of this work is to address the need for a paradigm shift in understanding and addressing users' privacy risks in the context of online social network with a specific focus on the third-party applications. Toward this end, we first discuss related research regarding Facebook in Chapter 2. Then, we systematically examine how Facebook implement users’ information control in Chapter 3. We then collect data from 1800 most popular Facebook apps to figure out what kinds of personal information third-party apps are trying to obtain from users and their friends. Our results confirm that there is a large amount of users' personal
information transmitting from Facebook to third-party apps. We detail our findings in Chapter 4. We also develop our own Facebook application and conduct a series of experiments to observe third-party apps' practices for privacy notice and consent. We discuss our findings from these experiments in Chapter 5. In Chapter 6, we point out several problems that may exist in the current authentication dialogs and propose two new designs for the authentication dialogs in hoping to address those problems. We then conduct a preliminary user study to evaluate our new designs, and summarize this study and discuss the results in Chapter 7. Chapter 8 concludes this thesis with discussions on the future research directions.
Chapter 2

Related Work

Recently, the booming popularity of Facebook has attracted significant attention. Facebook has become one of the fundamental mediums and tools for social interactions, involving high-volume of information exchange activities. Based on this high-volume of information that users have shared on Facebook, some researchers conducted research that focused on understanding users’ behavior in the age of Facebook. For example, Dugan and his colleagues reported an alternative way for users to richly describe themselves on Facebook (Dugan et al., 2008). Barkhuus and Tashiro did research regarding how student socialized in the age of Facebook (Barkhuus & Tashiro, 2010).

The intensive propagation of personal data also introduces a variety of privacy risks for users of Facebook. Some research regarding Facebook privacy and security issues stays at the descriptive level. For example, Gross and Acquisti (2005) present their findings on general usage pattern of Facebook; the distribution of privacy concern across gender, membership status, and user age; as well as the users’ awareness of Facebook’s privacy control options (Gross & Acquisti, 2005). In addition to such descriptive level of research, prior privacy research also identified a wide range of privacy threats associated with the use of Facebook, such as accidental information disclosure, damaged reputation and image, unwanted stalking, and reconstruction of users’ identities (Boyd & Ellison, 2008; Debatin, Lovejoy, Horn, & Hughes, 2009; Gross & Acquisti, 2005). Further, an additional dimension that represents the complexity of studying privacy risks on Facebook is added by the large amount of information interactions between
third-parties and Facebook users, which we consider as the unauthorized use of personal data by third-parties. As one recent Wall Street Journal pointed out, there were numerous third-party apps on Facebook transmitting identifiable users’ information out of this platform to advertising companies (Steel & Fowler, 2010).

To the best of our knowledge, there is little research to address the privacy threats associated with the use of Facebook third-party apps. The only exception is the research conducted by Lipford and her colleagues, which aims to provide users a better visualization of the third-party apps’ information accessing and publishing practices. In doing so, users might have a better awareness in terms of how the app will use their information and thus users might be able to avoid some undesirable information leakage. Lipford et al. (2008) designed an interface with a better audience view to help people understand Facebook’s privacy settings (Lipford, Besmer, & Watson, 2008). In critiquing Facebook’s available privacy control options, they identified some design flaws that might lead to users’ misunderstandings. However, Lipford et al. (2008) did not propose any actionable solution or approach to better educate or inform users in terms of what they can do to limit apps' data access and restrict apps' publishing ability during the process of adding the apps to their profiles. Further, Lipford et al. (2008) did not examine the circumstances under which users’ privacy settings could be violated by third-party apps and alert users when these violations happen. To address these gaps in the literature, we aim to provide Facebook users: 1) with better control options to limit third-party apps' data access and restrict apps' publishing ability on Facebook, and 2) with better alert mechanisms to inform users under the circumstances when users’ privacy settings are violated by third-party apps.
Chapter 3

Overview of Users’ Information Control on Facebook

Users’ Information Control on Facebook

On Facebook, the only way users could limit others’ access to their shared contents is to adjust their privacy settings. By doing so, Facebook users could control who can access what types of shared contents on Facebook. Figure 3-1 shows the user interface associated with privacy settings on Facebook. Facebook also provides detailed explanations of these privacy settings\(^1\).

![Figure 3-1. User Interface of Privacy Settings on Facebook.](http://www.facebook.com/#!/privacy/explanation.php)
Information Control Between Facebook Users and Third-Party Apps

Facebook platform now is mainly using OAuth 2.0 protocol to limit the third-party applications’ information accessibility. Specifically, OAuth 2.0 is used for third-party authentication and authorization. The goal of this protocol is to address the issues brought by the traditional client-server authentication model, in which the client can access a protected resource on the server by authenticating with the server using the resource owner’s credentials. OAuth adds an authorization layer and separates the role of the client (third-party application) from that of the resource owner (Facebook user) (Hammer-Lahav, Recordon, & Hardt, 2011). Figure 3-2 demonstrates the flow of this protocol.

Figure 3-2. The OAuth 2.0 protocol.

---

2 See URL: http://developers.facebook.com/docs/authentication/
Under this protocol, when a user wants to add an application to her Facebook profile, and that application wants to access the user’s data from Facebook platform, the application needs to ask the user for authorizations. By default, the user is asked to authorize the app to access her basic information that is available publicly or by default on Facebook. If the app needs more than this basic information to function, the app would request specific permissions from the user.

**User Interface.**

Figure 3-3 shows the user interface associated with the application authentication. In this OAuth dialog, the first category “access my basic information” will always show the default information that will be accessed by the application. As shown in Figure 3-3 below, this category includes basic user information such as name, profile picture, gender, network, user ID, list of friends, and any other information the user has shared with everyone. In addition to the category of “basic information”, the apps could also ask for extended permissions to access more user data (e.g., contact information, photos and videos, etc.) or behave on behalf of users to post on their walls.
Data Permissions Defined in Developers’ Source Codes versus Shown in User Interface.

To compare the developer’s view versus the user’s view in terms of publishing permissions, data access permissions from users and their friends’ information, we use PHP SDK provided by Facebook to develop our own application named as “Permission Experiment” and test all the extended permissions that could be requested by the application. The results, conducted on Mac OS X 10.5.8 using a Firefox browser, are summarized in Table 3-1, 3-2, and 3-

---

This software development kit (SDK) provides Facebook Platform support to my PHP-based web apps. This library helps me add Facebook Login and Graph API support to my Website.
3. In below tables, we list all the parameters developers of the apps would ask for extended permission in their source code in the first column. In the second column, we list descriptions that Facebook provides to developers regarding these extended permissions. The third and fourth columns are the category name and description that will be displayed in the OAuth dialog and shown to users.

**Table 3-1. Contents of Publishing Permissions: Developer View versus User View**

<table>
<thead>
<tr>
<th>Developer View of Permission</th>
<th>Description for Developer</th>
<th>User View of Permission</th>
<th>Description for User</th>
</tr>
</thead>
<tbody>
<tr>
<td>publish_stream</td>
<td>Enables your application to post content, comments, and likes to a user's stream and to the streams of the user's friends.</td>
<td>Post to my Wall</td>
<td>The application may post status messages, notes, photos, and videos to my Wall</td>
</tr>
<tr>
<td>sms</td>
<td>Enables your application to send messages to the user and respond to messages from the user via text message</td>
<td>Send me SMS messages</td>
<td>The application may send SMS messages to my phone</td>
</tr>
<tr>
<td>offline_access</td>
<td>Enables your application to perform authorized requests on behalf of the user at any time.</td>
<td>Access my data any time</td>
<td>The application may access my data when I'm not using the application</td>
</tr>
<tr>
<td>publish_checkins</td>
<td>Enables your application to perform checkins on behalf of the user</td>
<td>Manage my pages</td>
<td>The application may login as one of the my Pages</td>
</tr>
</tbody>
</table>
Table 3-2. Contents of Data Permissions for Users: Developer View versus User View

<table>
<thead>
<tr>
<th>Developer View of Permission</th>
<th>Description for Developer</th>
<th>User View of Permission</th>
<th>Description for User</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_about_me</td>
<td>Provides access to the corresponding information as certain property or connection</td>
<td>Access my profile information</td>
<td>Details regarding information the application may access would be listed for description.</td>
</tr>
<tr>
<td>user_activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_birthday</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_education_history</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_events</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_hometown</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_interests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_likes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_notes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_religion_politics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_website</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_work_history</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read_insights</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_online_presence</td>
<td>Provides access to the user's online/offline presence</td>
<td>Online Presence</td>
<td>No description</td>
</tr>
<tr>
<td>user_photo_video_tags</td>
<td>Provides access to the photos/videos the user has been tagged in or uploaded</td>
<td>Access my photos and videos</td>
<td>Details regarding information the application may access would be listed for description.</td>
</tr>
<tr>
<td>user_photos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_videos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_relationships</td>
<td>Provides access to the user's family and personal relationships and relationship status and relationship preferences</td>
<td>Access my family &amp; relationships</td>
<td>Details regarding information the application may access would be listed for description.</td>
</tr>
<tr>
<td>user_relationship_details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Provides access to the user's primary email address in the email property</td>
<td>Send me email</td>
<td>The application may email me directly.</td>
</tr>
<tr>
<td>read_stream</td>
<td>Provides access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed</td>
<td>Access posts in my News Feed</td>
<td>No description</td>
</tr>
<tr>
<td>xmpp_login</td>
<td>Provides applications that integrate with Facebook Chat the ability to log in users.</td>
<td>Access Facebook Chat</td>
<td>No description</td>
</tr>
</tbody>
</table>
Table 3-3. Contents of Data Permissions for Users’ Friends’ Information: Developer View versus User View

<table>
<thead>
<tr>
<th>Developer View of Permission</th>
<th>Description for Developer</th>
<th>User View of Permission</th>
<th>Description for User</th>
</tr>
</thead>
<tbody>
<tr>
<td>friends_about_me</td>
<td>Provides access to the corresponding information as certain property or connection</td>
<td>Access my friends’ information</td>
<td>Details regarding information the application may access would be listed for description.</td>
</tr>
<tr>
<td>friends_activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_birthday</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_education_history</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_events</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_hometown</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_interests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_likes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_notes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_online_presence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_photo_video_tags</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_photos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_relationships</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_relationship_details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_religion_politics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_videos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_website</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>friends_work_history</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In Facebook privacy settings, there is a section called Apps and Websites. After the installation of apps, this section is supposed to help users control the information sharing between them and external websites or third-party apps. However, the current design of this section on Facebook can only allow users to partially control the information that will be accessed by apps after their installation of third-party apps. Users cannot freely remove the information requested by the Apps and Websites settings. Some of the information required by third-party apps is even un-removable (Figure 3-4).
Graph API

In addition to analyzing the among-users and users-apps information control, we also need to understand the bridges between the users’ information and third-party. In other words, we need to know via what mechanism, Facebook third-party apps could access users’ information. Thus, in this section, we take a closer look at the Graph API system by calling which developers could access users’ information.

Basically, the Facebook Graph API system is object-based, for example, Album, Application, Comment, Event, Photo, Video, etc., are all objects. The Graph API system could consistently represent objects and the connections between objects in the social graph. All of them present a simple and consistent view of the Facebook social graph.4

Every object in Facebook has an unique ID. Developers can access the properties of an object by requesting its ID such as “http://graph.facebook.com/ID”. And to successfully fetch such properties by this API, some extended permissions might be required. In addition to get object properties, the Graph API also provides a method to access the connections among

---
4 See this URL: http://developers.facebook.com/docs/reference/api/
different objects. There are several different types of connections. And developers can examine certain types of connections of an object by invoking `http://graph.facebook.com/ID/CONNECTION_TYPE`. Similar to properties, some of the connections may also ask for corresponding extended permissions.

Another group of Graph APIs can perform the function of publishing information to certain user profile location. In order to get these APIs work, we have to ensure that the “publish_stream” permission for some objects (e.g. photo, post, etc.) are granted by the user.

So far, we have discussed the information control implementations on Facebook. In the next Chapter, we will discuss what kinds of users’ personal information are accessed by third-party apps.
Chapter 4
Overview of Facebook Third-party Apps

In this section, we discuss about what kinds of users’ information are released to third-party beyond the Facebook platform.

From the Facebook application directory, we could locate the URLs for the most popular 1800 applications in 9 categories. These 9 categories are business, education, entertainment, friends & family, games, just for fun, lifestyle, sports, and utilities. We collected data from top 200 most popular applications for each category. By going through the list of these applications, we get the profile page URL for each application. Then we use the software “Locoyspider” to collect and save data from web pages, with the number of monthly active users for these 1800 applications from their profile pages. Next we use the list of “Go to App” URLs to either access the “Request for permission” authentication dialog which lists all the information that the application requests access from users, or to be redirected to an application’s external page. We only consider the applications that would pop-up a “Request for Permission” dialog after clicking the “Go to App” button. From these authentication dialogs, we capture the types of information an application is requesting access from users. Combining this information (types of information requests) with the number of monthly active users for each application, we can count how many times a certain type of information is released to certain application within a month.

The data collection was completed at the end of December 2010. Among those 1800 most popular applications, there were 1305 applications displaying authentication dialogs when they requested data access from users. From the end user’s perspective, there are 12 types of information requested by the authentication dialog. For each type of these requests, we can first
get a list of applications that require it. We sum up the number of monthly active users for each application on the list to get the total number of users who are requested for this type of information. We treat this total number as the total times that such user information is requested per month.

The results of our data releasing measurement experiment are shown in Table 4-1 and Figure 4-1. We found by that time, almost 900 million person times were asked to release the basic information to applications. And the top three most frequently released users’ information or rights are those belonging to “Send me email”, “Access my profile information”, and “Post to my Wall” categories.

Table 4-1. Users’ Information Releasing Description.

<table>
<thead>
<tr>
<th>Data Category</th>
<th>No. of programs request for the data</th>
<th>Total times of user information are requested by apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send me email</td>
<td>454</td>
<td>238,991,048</td>
</tr>
<tr>
<td>Post to my wall</td>
<td>670</td>
<td>137,473,280</td>
</tr>
<tr>
<td>Access my profile information*</td>
<td>148</td>
<td>178,912,316</td>
</tr>
<tr>
<td>Access my data any time</td>
<td>76</td>
<td>17,450,664</td>
</tr>
<tr>
<td>Manage my pages</td>
<td>8</td>
<td>237,067</td>
</tr>
<tr>
<td>Access my photos and videos</td>
<td>128</td>
<td>43,227,008</td>
</tr>
<tr>
<td>Access my friends information</td>
<td>148</td>
<td>68,436,680</td>
</tr>
<tr>
<td>Access posts in my News Feed</td>
<td>66</td>
<td>30,635,352</td>
</tr>
<tr>
<td>Online Presence</td>
<td>16</td>
<td>4,003,824</td>
</tr>
<tr>
<td>Access my family &amp; relationship</td>
<td>28</td>
<td>6,617,296</td>
</tr>
<tr>
<td>Access Facebook Chat</td>
<td>8</td>
<td>1,739,160</td>
</tr>
<tr>
<td>Send me SMS messages</td>
<td>10</td>
<td>1,195,720</td>
</tr>
</tbody>
</table>

* The users’ information accessed by this category may vary according to different app requests.
In addition, we also counted the numbers of different types of information requests within each application category defined by Facebook and tried to find out the correlation between the types of application and information requests. However there is no significant pattern discovered. In Table 4-2, we listed the basic data request summary.

More questions arose during our process of analyzing the overall information control implementations and privacy practices by those 1800 popular Facebook apps, we list those questions below:

- Who can control the display and content of the authentication dialog for privacy notice and consent?

- Can users exercise control over limiting the third-party apps' information access or publishing ability?

- To which extend could the third-party apps override users' global privacy settings on Facebook?

**Figure 4-1. Users’ Personal Information Accessed by Third-Party Applications.**
To which extent would the authentication dialog truly reflect the third-party apps' information practices?

Table 4-2. Summary of Different Type of Applications and Their Information Requests.

<table>
<thead>
<tr>
<th>Category</th>
<th>Request for permission</th>
<th>Access my basic information</th>
<th>Send me an email</th>
<th>Access my profile information</th>
<th>Post to my Wall</th>
<th>Manage my profiles and videos</th>
<th>Access posts in my News Feed</th>
<th>Access my family &amp; related people</th>
<th>Send me SMS messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1306</td>
<td>1305</td>
<td>227</td>
<td>335</td>
<td>38</td>
<td>129</td>
<td>4</td>
<td>64</td>
<td>74</td>
</tr>
<tr>
<td>Business</td>
<td>101</td>
<td>101</td>
<td>16</td>
<td>13</td>
<td>3</td>
<td>9</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Education</td>
<td>118</td>
<td>118</td>
<td>17</td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Entertainment</td>
<td>135</td>
<td>135</td>
<td>21</td>
<td>37</td>
<td>7</td>
<td>17</td>
<td>0</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>Friends &amp; Family</td>
<td>158</td>
<td>158</td>
<td>30</td>
<td>76</td>
<td>4</td>
<td>13</td>
<td>0</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Games</td>
<td>191</td>
<td>191</td>
<td>42</td>
<td>20</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Just For Fun</td>
<td>156</td>
<td>156</td>
<td>25</td>
<td>52</td>
<td>8</td>
<td>18</td>
<td>0</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Lifestyle</td>
<td>155</td>
<td>155</td>
<td>40</td>
<td>63</td>
<td>10</td>
<td>35</td>
<td>1</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>Sports</td>
<td>162</td>
<td>162</td>
<td>72</td>
<td>26</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Utilities</td>
<td>129</td>
<td>129</td>
<td>14</td>
<td>25</td>
<td>5</td>
<td>13</td>
<td>1</td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

* The users’ information accessed by this category may vary according to different app requests.
Chapter 5

Third-party Apps' Practices for Privacy Notice and Consent

Given the complexity of users’ information control on Facebook and the large amounts of information requests from third-party apps, we need to carefully look into the current privacy notice and consent practices by third-party apps on Facebook. We developed our own Facebook app “Permission Experiment” and performed a series of tests to address those 4 questions we proposed earlier:

- Our first test is based on our own Facebook application “Permission Experiment”. We tested when the developers add different extended permissions to their source code. How the display of the authentication would change.

- Our second test is based on the Facebook privacy settings for Websites and Apps. We observed and tested whether users could remove certain information request when they install the app and after they install it.

- Our third test is based on two applications. The first is the “Happy Calendar 2011” and the second is “Permission Experiment” developed by ourselves. We tested when the user’s privacy settings make certain information not seen by everyone, whether the application’s information access and publish would violate user’s privacy settings.

- Our forth test is also based on the application “Permission Experiment”. In this study, we tested what information could be accessed by the application with extended permission.

We will report the corresponding results in the next four sections.
A display test

We found that if the developers change their source code to ask for different permission to access users’ personal information or publishing ability, the authentication dialog will change correspondingly and sometimes the display will be chaotic. For example, when the app is asking to access photos and videos the user’s friends have uploaded and been tagged in at the same time, the display of these permissions would look confusing, as shown in Figure 4-1.

![Request for Permission](image)

**Figure 5-1.** Screenshot of a Facebook Application Requesting Access to User’s Photos and Videos and Friends’ Photos and Videos.

As shown above, we assume from this dialog that users would feel confused by the sentence “Photos, Videos and Photos and Videos of Them” marked by the red line, which seems not a correct English sentence in grammar. Thus it might be hard for users to directly understand what information regarding their friends is going to be accessed by the application. Such problem is not solely caused by grammar. Even if the permission statement is expressed correctly in grammar, as that expressed under the “Access my photos and videos” subtitle, the users may still
not be able to figure out the difference between “Photos Uploaded by Me, Videos Uploaded by Me” and “Photos and Videos of Me” in case he is a novice user to Facebook.

**A limitation test**

In the current design of the authentication dialog, we found that there is no way for users to limit the apps' information access or publishing ability during the installation process. Even the post installation information settings in “settings for Websites and Apps” cannot sufficiently help users to control what information to share with apps.

**A privacy violation test**

Users on Facebook could customize their privacy settings for certain information. For each piece of a user’s personal information, the user can specify a list of users who can access to it. This test is designed to tell whether certain information is actually protected and only can be seen by the appointed user(s).

We started by developing our own Facebook application using the PHP SDK provided by Facebook. Later, we create a fake Facebook account “A” and customize A’s privacy settings. Then we use an application “Happy Calendar 2011”, as well as our “Permission Experiment” application, to test the accessibility of A’s private information from these two applications and whether there exists violation of A’s privacy.

After running the tests, we discovered that when the user grants the application permissions to access certain part of her profile, no matter what is the privacy setting for that part,
the application could access the content. If the application also asks for the “publish_stream” permission, with which the application could post content, comments, and likes to a user's stream and to the streams of the user's friends and could publish content to a user's feed at any time, the user’s privacy may be violated. We give an example.

- User A does not want anyone else to know her birthday. So she sets the privacy setting for that as “Only me”, which means her birthday cannot be seen by other users on Facebook except herself. However, when she adds the application “Happy Calendar 2011” to her profile, whose description is “Want to keep track of your friends' birthday? Show your friends who's having a birthday each month with Happy Calendar!”, she is asked to grant the app permissions to access her birthday and her friends’ birthday and to publish on stream. Without knowing the risk of privacy disclosure, user A grants the app all the permissions. Later, user A finds “Happy Calendar 2011” creates an album and posts all her friends’ birthdays that she can access, as well as her own, in a calendar with their profile pictures marking in the corresponding dates. Moreover all A’s friends can access that album. And they get a new post in their feed as the album is created. As a result the information “birthday”, which A wants to keep secret, could now be accessed by her friends on Facebook. And we report this as a privacy violation.

In the above scenario, we only use “birthday” as an example to give out some general ideas regarding how the private information could be released by an application. Virtually, the real situation is even worse. As long as the application asks for the permissions to access the user’s or/and her friends’ data, to publish on stream or other publishing permissions, and user grants those permissions, not only the user’s profile information like “birthday” but also other contents such as photos, videos, comments, etc., actually everything she has shared on Facebook, could be accessed and released by that application. Here, we even did not touch any hot debate
regarding third-party applications collecting and selling Facebook users data to Ad companies. Only lock our focus within Facebook platform, we could find privacy violation due to the conflict between users’ privacy settings and applications’ data collecting and publishing practices. Or we say these are the conflicts between users’ privacy settings and Facebook’s powerful APIs that enable application developers to collect and publish all kinds of users’ data. The whole disclosure process is shown as following.

![Diagram showing conflicts between users' privacy settings and Facebook APIs]

**Figure 5-2. The Process of The App Discloser User’s Private Information.**

**A reflection test**

In this study, we use our application “Permission Experiment” to ask for different extended permissions from user A and test what users’ information could be accessed by the corresponding permission being granted.
After running the information access experiment tests with our application “Permission Experiment” we discovered that sometimes the prompting message displays in the authentication dialog might not sufficient for users to understand what information in their profile will be accessed by the application. If one application asks for the grant of extended permissions to access a certain object, with that permission in hand, the application can access not only all of its non-permission required properties but also its connected objects’ properties which are not required for more permissions. Furthermore, if the second-level objects are connected to the third-level objects that are not required for more permission, those objects’ properties are still available to the application. And this information access chain will not stop until it reaches an object that does not have any further object connecting to it.

We give an example:

- When the application “Permission Experiment” only asks for extended permission “user_photos”, users will see the following authentication dialog when they add the app. In this dialog window, with the category title “Access my photos and videos”, there is only one simple and short phrase, “Photos uploaded by me”, used for describing that the extra user information could be accessed by that app. From this prompting message, users might easily holds the idea that only the photos they have shared on Facebook would be access by that app. However, in fact, with this simple “user_photos” permission being granted, the real amount of information that app could access is far more beyond the photos themselves. More specifically, the “user_photos” permission actually enables the app to access all albums objects the user has created. For each album object, it has 10 properties and 3 connected objects (photo, comment, and picture) which are all non-permission required. And for those 3 connected components, both photo and comment have there own properties and following connected objects, which distribute this permission further. So, the actual information that could be accessed by allowing the
Therefore, we could summarize our preliminary findings:

- The developers of third-party apps can control the display and content of the authentication dialog for privacy notice and consent. The content of the dialog will be determined by the types of extended permissions developers are requested to access users' personal information or publish on users' walls.

- During the process of adding the apps to their profiles, users do not have any control to limit apps' access to their information or restrict apps' publishing ability. But after they add the apps, users can edit some categories of information access or publishing ability via adjusting their privacy settings.
- There is conflict between a user's privacy setting and a third-party app's data practice. In other words, Facebook's powerful APIs could enable third-party apps to override users' privacy preferences expressed through their privacy settings.

- The prompting message for privacy notice and consent displayed in the authentication dialog may not be sufficient for users to understand what information in their profile will be accessed by the app.
Chapter 6

Proposed Designs

Problems with the current authentication dialog (AD)

In the previous chapter, both the statistical analysis of apps' information request and the following tests on the apps' privacy notice and consent practices have brought us some insights for Facebook third-party apps' information accessing and publishing practices. Our previous research shows that there was a large amount of user information transmitting from Facebook to external entities. In terms of the third-party apps’ current practices for obtaining privacy consents from users, an authentication dialog is usually generated by an app for the purposes of gaining data permissions from users and their friends.

Based on the analysis of the current authentication dialog for Facebook third-party apps, we identified three major problems we hope to address with the current design of authentication dialog:

**Problem 1**

Below is the screenshot of a Facebook app’s authentication dialog. This app is asking for publishing permissions and data permissions at the same time. In this case, users may not be able to distinguish them and do not know how the app will use the information.
Problem 2

During the process of adding the apps to their profiles, users do not have any control to limit apps’ access to their information or restrict apps’ publishing ability. But after they add the apps, users can edit some categories of information access or publishing ability via adjusting their privacy settings.

Problem 3

There may be conflict exists between a user’s privacy settings and a third-party app’s data practice. In other words, Facebook’s powerful APIs could enable third-party apps to override users’ privacy preferences expressed through their privacy settings.
Design Principles

Smith et al. suggested that there are six managerial action areas associated with information privacy (Smith, 2004). Out of those six, there are four areas that would affect individuals’ concern about organizational privacy practices: 1) collection of personal information; 2) unauthorized secondary use of personal information; 3) errors in personal information; and 4) improper access to personal information (Smith, Milberg, & Burke, 1996). Now we could apply this framework to Facebook users’ concern about third-party applications’ information accessing and publishing practices. First of all, we regard that Facebook user’s information is all uploaded by user herself. We then can claim the third error concern may not be a primary concern in this context. Second, user’s unauthorized secondary use concern should be one of the primary concerns within the Facebook third-party apps’ context. Because, as the Wall Street Journal article (Steel & Fowler, 2010) pointed out, numerous popular apps are transmitting users identifiable information to advertising companies. Meanwhile, we believe this dimension of user’s concern could be reduced if we limit the third-party apps’ information accessing and publishing abilities. Because in this way, the third-party apps would not have the ability to access as much users’ information as they want and then they could not share those information with other companies outside Facebook. In other words, if we could control third-party apps’ collection of personal information and improper access to personal information, we could reduce people’s concern regarding unauthorized secondary use. And then in generally alleviate users’ concern about third-party applications’ information accessing and publishing practices.

If we take a look at those three problems regarding current Facebook third-party applications mentioned before. We find that the first and second problems can be categorized as collection concern, and the third problem can be categorized as the improper access concern. Thus we believe, if we could address these three problems existing in the current Facebook third-
party applications authentication dialog, we would effectively alleviate Facebook users’ concern regarding third-party applications information accessing and publishing practices.

Many studies have been done on empowering user control over limiting information disclosure (Bruns, 2003; Shackel, 1991). These solutions mainly aim at addressing the collection concern. Based on these studies, and aiming to address the first two problems, here we propose the following two design principles:

**Principle 1**

The authentication dialog should provide explicit signals for users to distinguish what data would be accessed by the app and how the data would be used.

**Principle 2**

The authentication dialog should provide options for users to control the information accessibility or publishing ability before adding the app to the user’s Facebook profile.

To address the third problem we found in our privacy violation test, which tells that peoples’ privacy settings might be overridden by apps’ information accessing and publishing practices, we proposed the third design principle as following.

**Principle 3**

The authentication dialog should provide alert signals for users when data and publishing permissions requested by the app will violate the users’ privacy settings.
These design principles fall into different perspectives, including both end-users on OSNs and service providers of OSNs. As we see in the description of current problems of authentication dialog, the first three design principles should already enough for addressing them. However, here, we want to go one step further, and test whether users want the authentication dialog to reflect their privacy settings. In order to figure out the necessity for the forth design principle, we tend not to package all the principles to generate one new design. Instead, we presented two new designs here for a more clear-cut analysis.

**Principle 4**

The authentication dialog should reflect a user’s current privacy settings.

**Alternative Authentication Dialogs**

In the last nineteen year, the nutrition label has become iconic and ubiquitous (Administration, 1994). Kelley and her colleagues developed a privacy label that presents to consumers the ways organizations collect, use, and share personal information based on the nutrition label (P. G. Kelley, Bresee, Cranor, & Reeder, 2009). In their design, they adopted several general principles form the nutrition labeling literature to address problems with the Expandable Grid (P. Kelley, McDonald, Reeder, & Cranor, 2007): 1) to emphasis the group labels by a box so that the users can identify different sets of information; 2) to use bold rules to separate sets of information in order to expedite the users navigation through the list; 3) to have a bold and clear title to inform the user the purpose of the information listed (Administration, 1994;
And their design helps people gain a better understanding about privacy policies. To provide Facebook users a better indication about what kinds’ of their information would be used by apps. Our authentication dialog designs in this thesis adopt a similar set of considerations. In addition to these principles, we try to consider some design factors from the Human Computer Interaction (HCI) theories. Carroll mentioned in his book (Carroll, 2003) that “people rely on analogies with familiar, readily envisaged domains to build mental models of less-familiar, less-visible domains”. Following this implication, we deliver some icons and color themes that are well consistent with users’ already built mental models in daily life on our dialog design. For instance, we use the red exclamation mark to indicate there is a conflict happening, which is corresponding to most users’ experience that such mark is sign for alert. More design details are listed in Table 6-1. Such design is approved by the majority of subjects in our user study, which will be discussed later in this thesis.

Envisioned by design principles and previous discussions, we present our alternative designs for third-party applications’ authentication on Facebook. As highlighted earlier, we aim to present interfaces representing different aspects derived from design principles. The reason of doing so is because we want to figure out whether users want the authentication dialog to reflect their privacy settings. Thus, we provide two solutions, and we are interested in users’ comments on these two new designs of authentication dialog.

Below we present two new designs for the Facebook third-party apps’ authentication dialog, as shown in Figure 3 and Figure 4. We present the design elements Table 5-1.
Table 6-1. The Design Elements.

- **1. The layout of permissions.** We list all the data required (basic information and data permissions) by the app in the first column and how the app will use the information (including publishing permissions) in the first row.

- **2. The tick mark and checkbox.**
  - Un-clickable tick marks represent corresponding information will be accessed by the app and used in some ways. You cannot control it.

  - Check boxes represent you could control whether you would allow the app to access and use your corresponding information.
    - When the check box is **checked**: you allow the app to access certain information and use it.
    - When the check box is **un-checked**: you do not allow the app to access the corresponding information or use it.

- **3. The exclamation point design.** The red exclamation point is designed to alert you of potential privacy conflict. When the current information requested by the app conflicts with your privacy settings, this red exclamation point will alert you about that.

- **4. The extra buttons.** We added two buttons to help the user control how the application accesses and publishes information.
  - **Follow My Privacy Settings** By clicking this button, all the check boxes with the red exclamation point alert will be unchecked, This means that the app will not be allowed to use this information.
  - **Uncheck All** By clicking this button, all the check boxes will be uncheck. Only the required amount of information will be shared with the app.

- **5. The color themes.** (Used for design proposal 2-POLY) We adopted three color schemes in our design to reflect the current privacy setting for those information requested by the app:
  - **GREEN** indicates current privacy setting for the corresponding information is “Everyone” and it will NOT be violated by adding app to your account.
  - **RED** indicates current privacy setting for that information is “Only Me” or “Specific People…” and it will be violated by adding the app.
  - **YELLOW** indicates current privacy setting for that information is something beyond “Everyone”, “Specific People…” or “Only Me”. That means the global privacy setting for that information may be violated by the app.
Monochrome authentication dialog (MONO)

Our first design of the authentication dialog is trying to fulfill the first three design principles. Our first authentication dialog is shown in Figure 5-2.

Figure 6-2. A New Monochrome Interface Design for Facebook Third-Party Authentication.
Polychrome authentication dialog (POLY)

Our second design of the authentication dialog, PLOY design, is an upgraded version of the MONO design. With all the functions in the MONO design being kept, the POLY design adopts a three-color scheme system to reflect users’ privacy setting. It is shown in Figure 5-3.

Figure 6-3. A New Polychrome Interface Design for Facebook Third-Party Authentication.
Chapter 7

User Evaluation

In this section, we present our user study to evaluate our MONO and POLY designs for the authentication dialog. In order to probe users’ opinions of and attitudes towards our designs, we adopted a qualitative method utilizing a structured questionnaire with open ended questions.

Participants

Participants were recruited from undergraduate classes at a public university in the United States. We specified that participants must be active Facebook users. Five extra credit points were awarded for their participations in this study. Students who chose to participate in the study remained staying in the classroom. There were in total 11 participants who participated in this user study. As the first step of this study (one week before participating the user study), participants were given a talk by the researcher that introduces the privacy problems regarding third-party applications on Facebook.

Questionnaires

After participants have a good understanding of the current privacy issues regarding third-party application on Facebook, we conducted a qualitative study presented as a questionnaire. Focusing on evaluating our MONO and POLY designs, our questionnaire was
composed with open ended questions. The questionnaire was designed to evaluate our new designs from following perspectives:

- Whether the design principles are sufficient to address users’ privacy concerns toward Facebook third-party apps?
- Whether the proposed designs achieve the claimed design principles?
- Whether users want the authentication dialog to reflect their Facebook privacy settings? Could those privacy settings be reflected by our POLY design?
- How do users perceive the effectiveness of our new designs for information control and privacy conflict alert?

In our actual user study, we asked users to critique the four design principles we proposed for address users’ privacy concerns towards Facebook third-party apps and whether the proposed designs achieve the claimed design principles. Then we asked participants whether they want the authentication dialog to reflect their privacy settings on Facebook and to what extent our POLY design could reflect their privacy settings. Next participants were asked to compare the current authentication dialog, the MONO design and the POLY design, from multiple perspectives, including attractiveness of the interface, perceived effectiveness in information control ability, perceived effectiveness in alerting users about third-party apps override their privacy settings, and overall likability.
Discussion

As the first step, we examined participants’ responses to the open-ended questions and identified significant concepts and aspects through content analysis of their answers. We then applied a more thorough process to code their answers for in-depth analysis. In this procedure, we examined the patterns in subjects’ responses and attempted to correlate concepts generated in the coding process. By doing this, we expected to find out participants’ attitudes and preferences on the current Facebook apps' authentication dialog and our newly proposed MONO and POLY designs. More importantly, we expected these results could infer a better authentication dialog design in practice.

“In the Right Direction”

Most of our participants (N=10) stated they think the four principles presented are sufficient to address users’ privacy concerns towards Facebook third-party apps. And almost all participants (N=10) agreed the proposed designs achieve the claimed design principles. For example, one participant said:

“They address basic issues such as notifying whether or not the third-party app will violate previously established privacy settings. The principles do an excellent job informing the user about the consequences of using the application.”
While participants pointing out these four principles are an excellent first step in managing users’ privacy concerns towards Facebook third-party apps, they also mentioned more perspectives of how privacy should be addressed:

**Friends’ information**

Some participations (N=4) mentioned the ability for an application to gather information about one’s friends is another issue to be addressed, because the user’s “...friends never download or agreed to the application’s term” and the user “…dose not own the information.” If the user is not diligent about setting secure privacy settings, it is possible that those applications will be able to access their friends’ information. This is unfair for her friends who are proactive and try to make smart privacy choices.

**Information monitor**

Another participant mentioned “the information that is extracted from a user’s profile should be monitored” in a real time fashion. In this way, the user could quickly access when and what the information was used by the app and have a better control regarding the information leakage. Also the authentication dialog should inform the user “why the app need the information they take.”
Educating the user

One participant insisted "a very key and important phase is all about educating the user," which in his opinion is "the most important part."

Users need authentication dialog to reflect their privacy settings.

All the participants would like the authentication dialog to reflect their privacy settings. Most of the participants (N=9) stated that the color scheme implemented in the POLY design could reflect their privacy settings. One participant said his privacy settings are too strict to be reflected by the POLY design and one participant hoped to have every detail of his privacy setting in the authentication dialog.

Comparing Different Authentication Dialog Designs

Based on the review of responses from participants, we compared three authentication designs: 1) current design; 2) new MONO design; and 3) new POLY design. We developed the following comparison themes for these three authentication dialog designs. For each authentication dialog design, we compared participants’ responses on visual effects, perceived information control ability, perceived effectiveness in alerting third-party apps override users’ privacy settings, and overall likability. The comparison is shown in Table 6-1.

Table 7-1. Comparing Authentication Dialogs.

<table>
<thead>
<tr>
<th>Comparing Themes/Metrics</th>
<th>Authentication dialog designs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual Effects</td>
<td>Ability to grab users’ attention to personal information released to the app.</td>
</tr>
<tr>
<td>Perceived information control</td>
<td>Participants’ perceived effectiveness</td>
</tr>
</tbody>
</table>
ability of three authentication dialog designs in helping users better control the app’s information accessing and publishing practices.

| Perceived effectiveness in alerting third-party apps override users’ privacy settings | Participants’ perceived effectiveness of three authentication dialog designs in alerting about app’s override users’ privacy settings. |
| Overall likability | To what degree participants favor each authentication dialog. |

**Visual Effects**

*Both MONO and POLY are good at grabbing users’ attention.* When comparing the new MONO and POLY designs to the current authentication dialog. Three participants thought the new designs with the exclamation point in red were attention grabbing and they could show the users all of the information that the application is taking from him. They believed that if the new designs were implemented to Facebook, users will definitely pay more attention to their personal information security.

*MONO does a better job than POLY.* One participant believed that the MONO design does a better job than the POLY design. The major reason is that the introduction of the color in POLY is too distracting for users.

*POLY does a better job than MONO.* The majority of participants (N=7) believed that the POLY design dose a better job than the MONO design. In their responses, they stated that “*with the bright colors displayed on the request for permission page, it can’t help but draw attention.*”
Perceived information control ability

The majority of the participants (N=7) regarded the new designs could help users better control the app’s information accessing and publishing practices. They thought the check boxes and extra buttons place control in the hands of the users, rather than the apps. The users would have the option to remove some of the data collection by un-checking the permissions that the application has. Others (N=4) thought new designs would not help users better control the app’s information accessing and publishing practices. One of them mentioned the app developers could start to make more and more users’ information as required and that will lead to the Facebook users having less control in the long run. Another participant thought there seemed to be no added control of the information, only an added convenience and awareness.

Perceived effectiveness in alerting users that third-party apps override their privacy settings

The effectiveness of authentication dialog in alerting users that third-party apps override their privacy settings lies in multiple aspects. Similarly, in probing participants’ opinion regarding this issue, we obtained answers from various perspectives aside from the aspects of attention grabbing and control ability.

Most of the participants (N=8) regarded the new POLY design better in alerting users third-party apps overriding their privacy settings than the MONO design or the current authentication dialog. The major reason is derived from the fact that the new POLY design implemented the color scheme. These participants thought the POLY design is better because the information in this authentication dialog is highlighted by different colors based on users’ privacy settings. They argued that the POLY design shows the user how private the information was when the app wants access to it and is much easier for notices and conflicts to stand out than the
MONO design. Both the easy-to-see exclamation mark and red color, which is the universal signal for danger and problem, can help users be aware of the item where a conflict exists. Contrarily, the design in the current authentication dialog has no alert information when the users’ privacy setting conflicts with the app’s information accessing or publish practices.

Also two participants mentioned both the MONO and POLY designs would be useful as long as the users choose to take the time to learn the new system and pay attention to their recommendations. And one participant insisted that without educating and teaching users about what is happening to their personal information, none of the new design would work.

**Overall likability**

For participants who preferred POLY design rather than MONO (N=6), the major reason was the implementation of the color scheme that adapts to users’ privacy settings. The participants stated while both the MONO and the POLY design list the information in a more organized fashion and use the red exclamation point to alert users of the privacy conflict, and the POLY design is more eye-catching. The three-color schema could inform users about the potential threat of the violation. If something is red the users would think it is either a bad thing or a stop sign. That would make users think twice or at least try to read and understand how much information they may be allowing third-party apps to access.

On the contrary, some participants (N=4) thought the MONO design is more aesthetically pleasing and easier to understand. They stated the color of the POLY design would distract users and be overwhelming for users to view.
Chapter 8  
Conclusions and Future Work

The objective of this thesis is to understand the information economy created between social networking sites and third-party applications. Towards this end, we collect data from the 1800 most popular social apps from Facebook to analyze what kinds of personal information these applications are trying to obtain from users and their friends. We identify a number of challenges at the interface between the representation of material terms to the user and the underlying information collection and transmission mechanisms:

- During the process of adding the apps to their profiles, users do not have any control to limit apps' access to their information or restrict apps' publishing ability. But after they add the apps, users can edit some categories of information access or publishing ability via adjusting their privacy settings.

- There is conflict between a user's privacy setting and a third-party app's data practice. In other words, Facebook's powerful APIs could enable third-party apps to override users' privacy preferences expressed through their privacy settings.

- The prompting message for privacy notice and consent displayed in the authentication dialog may not be sufficient for users to understand what information in their profile will be accessed by the app.

To address these problems, we propose two new interfaces for the third-party app’s authentication dialog to: 1) empower user control to limit apps' data access and restrict apps' publishing ability during the process of adding the apps to their profiles, 2) alert users when their global privacy settings on Facebook are violated by the apps, and 3) help users better
understanding what kinds of their personal information will be accessed and used by the app. A user study was conducted to evaluate the authentication dialogs we proposed.

Based on the results of analyzing participants’ responses, we regard those two new designs meet the objectives we proposed in general. We also have gained the following insights into the design of Facebook third-party apps’ authentication dialog.

*Stand out to get noticed.* We found that users could be aware of the privacy conflict between their privacy settings and third-party apps’ information accessing and publishing practices only if they pay attention to the security cues spontaneously. Without achieving this goal, the authentication dialog could definitely fail in protecting users from privacy conflict. A well designed authentication dialog is perceived to do a better job in both alarming users of privacy conflict and enhancing users’ ability to avoid such conflict.

*Easy to understand.* According to participants’ suggestions for future design, the authentication dialog is supposed to be easy to understand. Users expect to understand what kinds of their information will be accessed and used by the app and whether there exists privacy conflict in a short time. Thus they could quickly make the decision whether to add the app to their profile. Therefore, the way to elaborate and interpret authentication information as well as users’ information control ability is crucial in interface design.

*Reflection of privacy settings vs. color scheme.* We found that all the participants wanted the authentication dialog to reflect their global privacy settings on Facebook. When they evaluated our color scheme implementation in POLY which is intended to reflect users’ privacy settings, some participants regarded it as an advantage. They argued the color scheme is eye-catching and to some extent can reflect their privacy settings. On the contrary, some participants regarded it as a disadvantage because they thought it would distract and be overwhelming to users. Thus, we consider the color scheme that we implemented in POLY design may not an
appropriate way to reflect users’ privacy settings. We need to find an alternative solution to achieve the corresponding function.

**Future work**

Through this Master thesis research, we further identified a number of topics that could be studied in the future.

First of all, as many studies pointed out, despite users expressing high concern about their privacy online, they do not always take action to protect themselves or their personal information. This phenomenon is known as the privacy paradox that users state high levels of privacy concerns but behave in ways that seemingly contradict to their privacy attitudes (Acquisti, 2004; Acquisti & Grossklags, 2005; Gross & Acquisti, 2005; Malhotra, Kim, & Agarwal, 2004). We should conduct a more realistic situation to evaluate studies to examine the performances of our proposed authentication dialogs in.

Furthermore, as there is a discrepancy between the information that the app claims to access and the actual amount information it obtained from the user. We could further develop a new authentication dialog, which could reflect all the information that will be accessed by granting certain permission.

Meanwhile, this thesis is mainly focused on the individual level of privacy issues related to third-party applications. We somehow did not consider how users’ friends’ behavior towards third-party apps could influence uses’ privacy. Future research could examine the collective privacy concerns related to third-party applications or users’ privacy settings. For example, another possible project we could conduct is to examine how a user’s privacy settings could be influenced by her friends.
We hope this thesis will motivate further research about users’ information control on social network platforms like Facebook.
Bibliography


